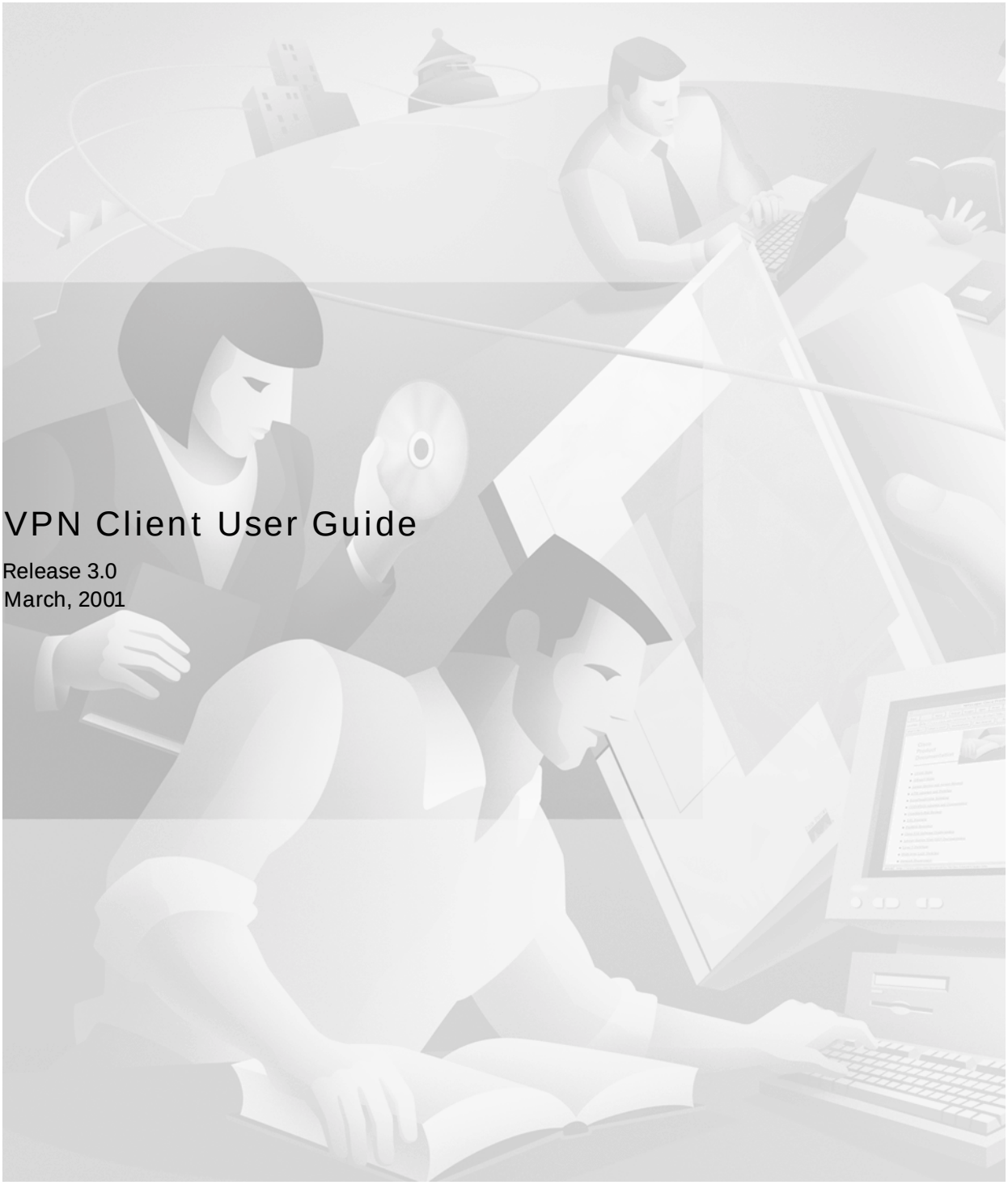


VPN Client User Guide

Release 3.0
March, 2001

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7812304=
Text Part Number: 78-12304-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco Net*Works* logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0011R)

VPN Client User Guide
Copyright © 2001, Cisco Systems, Inc.
All rights reserved.

Preface

About this manual ..... **ix**
Organization ..... **ix**
Additional documentation ..... **ix**
Other references ..... **x**
Documentation Conventions ..... **x**
Data Formats ..... **xi**
IP addresses ..... **xi**
Hostnames ..... **xi**
Usernames and Passwords ..... **xi**
Terminology ..... **xi**

1 Understanding the VPN Client

How it works **1-2**
Connection technologies **1-2**
Features **1-2**
VPN Client IPSec attributes **1-3**
Getting started **1-4**

2 Installing the VPN Client

Verifying system requirements **2-1**
Gathering information you need **2-2**
Installing the VPN Client **2-4**
What next? **2-5**

3 Configuring the VPN Client

How to get help **3-2**
Determining the VPN Client version **3-3**
What is a connection entry? **3-3**
How to create a new connection entry **3-4**
What next? **3-7**
Setting or changing connection entry properties **3-7**
Changing General settings **3-10**
Changing connection entry description **3-10**
Allowing IPSec through NAT mode **3-10**
Adjusting the peer response timeout **3-11**
Logging on to Microsoft Network (Windows 95, Windows 98, and Windows ME) **3-11**

Changing Authentication settings 3-11
Adjusting the peer response timeout 3-11
Logging on to Microsoft Network (Windows 95, Windows 98, and Windows ME) 3-11
Changing Authentication settings 3-11
Changing group name or group password 3-12
Selecting a different certificate 3-13
Changing Connection settings 3-13
Enabling and adding backup servers 3-14
Configuring a connection to the Internet via dial-up networking 3-14
Changing the VPN device address for a connection entry 3-16

4 Connecting to a private network

Starting the VPN Client 4-1
Connection procedure 4-2
Using the VPN Client to connect to the Internet via Dial-Up Networking 4-2
Authenticating to connect to the private network 4-3
User authentication 4-4
Authenticating via the VPN device internal server or RADIUS server 4-4
Authenticating via Windows NT Domain 4-5
Authenticating via RSA Data Security (RSA) SecurID 4-5
Using digital certificates 4-8
Completing the private network connection 4-9
Viewing connection status 4-9
IP security information 4-10
Connection statistics 4-10
Secured routes 4-11
Time connected 4-11
Resetting statistics 4-11
Closing the VPN Client 4-11
Disconnecting your VPN Client connection 4-12

5 Managing the VPN Client

Managing connection entries 5-2
Cloning a connection entry 5-3
Deleting a connection entry 5-3
Renaming a connection entry 5-4
Creating a shortcut for a connection entry 5-4
Importing a VPN Client Configuration File 5-4
Starting connections before logging on (Windows NT and Windows 2000 only) 5-6
What happens when you use Start Before Logon 5-6
Turning off Start Before Logon 5-7
Launching an application 5-7
Turning off Application Launcher 5-9
Viewing and managing the VPN Client event log 5-9
Starting the Log Viewer 5-9
Displaying the version of the software 5-10

Collecting events 5-10
Event# 5-11
Time 5-11
Date 5-11
Severity/type/level 5-11
Event Class/Message ID 5-11
Message text 5-11
Filtering events 5-11
Searching the log file 5-13
Printing the log file 5-13
Saving the log file 5-14
Clearing the events display 5-14
Installing a new version of the VPN Client 5-14
Uninstalling the VPN Client 5-15

6 Enrolling and managing certificates

Certificate stores -- what are they? 6-2
Enrolling for a certificate 6-2
Enrollment form 6-3
Starting enrollment 6-4
Enrolling via the network 6-5
Enrolling via a file request 6-7
Importing a certificate file 6-10
Managing personal and CA/RA certificates 6-11
Viewing a certificate 6-12
Verifying a certificate 6-13
Deleting a certificate 6-14
Changing the password on a personal certificate 6-15
Exporting a certificate 6-16
Managing enrollment requests 6-17
Viewing the enrollment request 6-18
Deleting an enrollment request 6-19
Changing the password on an enrollment request 6-19
Completing an enrollment request 6-20

A Copyrights and licenses

Client Software License Agreement of Cisco Systems 1
RSA software 2

Index

Figures

Figure 1-1: VPN Client applications 1-1
Figure 2-1: Initial VPN Client installation window 2-4
Figure 2-2: Setup Complete dialog box 2-5
Figure 3-1: Cisco Systems VPN Client program menu 3-2
Figure 3-2: Help button 3-2
Figure 3-3: Help menu 3-2
Figure 3-4: Displaying the VPN Client software version 3-3
Figure 3-5: VPN Client main dialog 3-4
Figure 3-6: New Connection Entry Wizard dialog 3-4
Figure 3-7: New Connection Entry Wizard dialog 2 3-5
Figure 3-8: New Connection Entry Wizard dialog 3 3-5
Figure 3-9: (Group) 3-6
Figure 3-10: **(Certificate)** 3-6
Figure 3-11: New Connection Entry Wizard dialog 4 3-7
Figure 3-12: VPN Client Options menu 3-8
Figure 3-13: Connection Entry Properties dialog (Windows 95 and Windows 98) 3-8
Figure 3-14: Connection Entry Properties dialog (Windows NT and Windows 2000) 3-9
Figure 3-15: Properties dialog > General tab 3-10
Figure 3-16: Properties dialog > Authentication tab 3-12
Figure 3-17: Reminder dialog 3-12
Figure 3-18: Selecting a certificate 3-13
Figure 3-19: Properties dialog > Connections tab 3-13
Figure 3-20: Backup server information dialog 3-14
Figure 3-21: Connect to the Internet via dial-up 3-15
Figure 3-22: VPN Client main dialog 3-16
Figure 3-23: Address change dialog 3-16
Figure 4-1: VPN Client main dialog 4-2
Figure 4-2: Dial-Up Networking User Information dialog 4-3
Figure 4-3: Confirming connections to ISP 4-3
Figure 4-4: Dial-Up Networking taskbar icon 4-3
Figure 4-5: Negotiating dialog 4-4
Figure 4-6: Internal or RADIUS server authentication dialog 4-4
Figure 4-7: Windows NT Domain authentication dialog 4-5
Figure 4-8: RSA authentication dialog 4-6
Figure 4-9: SoftID (Windows NT) authentication dialog 4-6
Figure 4-10: SecurID New PIN request 4-7
Figure 4-11: Entering a New PIN yourself 4-7
Figure 4-12: Accepting a PIN from the system 4-7
Figure 4-13: New PIN received 4-7
Figure 4-14: SecurID Next Cardcode mode dialog 4-8
Figure 4-15: Completing connection history 4-9
Figure 4-16: VPN Client Connection Status dialog 4-10
Figure 5-1: VPN Dialer Connect dialog 5-2
Figure 5-2: VPN Client Options menu 5-2
Figure 5-3: Clone Connection Entry dialog 5-3
Figure 5-4: Delete dialog 5-3
Figure 5-5: Rename Connection Entry dialog 5-4
Figure 5-6: Connection entry shortcut 5-4
Figure 5-7: Selecting a file to import 5-5
Figure 5-8: Importing the profile file 5-5
Figure 5-9: Import successful 5-5

Figure 5-10: Setting up Start Before Logon feature 5-6
Figure 5-11: Application Launcher option 5-8
Figure 5-12: Application Launcher dialog 5-8
Figure 5-13: Selecting an application 5-8
Figure 5-14: Starting the Log Viewer 5-9
Figure 5-15: Log viewer main window 5-10
Figure 5-16: Anatomy of an event message 5-10
Figure 5-17: Log Viewer Filter message 5-12
Figure 5-18: Searching the log display 5-13
Figure 5-19: Saving a log file 5-14
Figure 5-20: Uninstalling an existing version 5-15
Figure 5-21: Confirming the system restart 5-15
Figure 5-22: Running the Uninstall program 5-16
Figure 5-23: Confirming uninstall 5-16
Figure 5-24: Confirming your connections 5-16
Figure 5-25: Confirming your certificates 5-17
Figure 6-1: Selecting Certificate Manager 6-1
Figure 6-2: Certificate Manager main window 6-2
Figure 6-3: Enrollment Form 6-3
Figure 6-4: Protecting a certificate with a password 6-4
Figure 6-5: Selecting enrollment method 6-4
Figure 6-6: Entering network address 6-5
Figure 6-7: Enrollment summary 6-6
Figure 6-8: Certificate status messages 6-6
Figure 6-9: Resuming enrollment request 6-7
Figure 6-10: Receiving status update 6-7
Figure 6-11: Selecting file type and location 6-8
Figure 6-12: A PKCS10 certificate request 6-8
Figure 6-13: Specifying a filename 6-9
Figure 6-14: Enroll File Success message 6-9
Figure 6-15: File enrollment requests 6-10
Figure 6-16: Importing a certificate 6-10
Figure 6-17: Destination password for importing certificate 6-11
Figure 6-18: Certificate Manager Options menu 6-12
Figure 6-19: Displaying a Certificate 6-12
Figure 6-20: Verifying a certificate's validity 6-14
Figure 6-21: Entering password for deleting a certificate 6-15
Figure 6-22: Confirming deletion 6-15
Figure 6-23: Changing a certificate's password 6-16
Figure 6-24: Exporting a certificate 6-16
Figure 6-25: Export message 6-17
Figure 6-26: Managing enrollment requests 6-18
Figure 6-27: Viewing an enrollment request 6-18
Figure 6-28: Changing a certificate's password 6-19
Figure 6-29: Entering password to resume online enrollment 6-20

Tables

Table 2-1: VPN Client information worksheet 2-2
Table 5-1: Event types and severity levels 5-12
Table 5-2: Classes that generate events in the VPN Client 5-14

Preface

About this manual

This *VPN Client User Guide* tells you how to install, use, and manage the Cisco VPN Client with Cisco Systems products.

Organization

Chapter 1, *Understanding the VPN Client* briefly explains what the VPN Client is and how it works.

Chapter 2, *Installing the VPN Client* tells you how to install the VPN Client.

Chapter 3, *Configuring the VPN Client* tells you how to configure the VPN Client, including setting optional parameters.

Chapter 4, *Connecting to a private network* tells you how to connect to a private network using the VPN Client and an Internet connection.

Chapter 5, *Managing the VPN Client* tells you how to manage the VPN Client and its connections. This chapter also explains how to: install a new version, uninstall, reconfigure the VPN Client automatically, set the MTU size, and use the Log Viewer application.

Chapter 6, *Enrolling and managing certificates* tells you how to obtain digital certificates to use for authentication and how to manage these certificates on your system.

Appendix A, *Copyrights and licenses* provides copyright and license information for software that the VPN Client uses.

Additional documentation

The VPN Client includes an extensive online HTML-based help system that you can access through a browser in several ways: clicking the **Help** icon on the Cisco Systems VPN Client programs menu (**Start>Programs>Cisco Systems VPN Client>Help**), pressing F1 while using the applications, or clicking the **Help** button on screens that include it.

The *VPN Client Administrator Guide* tells how to configure a VPN 3000 Concentrator for remote user connections via the VPN Client, how to automate remote user profiles, how to use the VPN Client command line interface, and how to get troubleshooting information.

The *VPN 3000 Concentrator Series Getting Started* manual explains how to unpack and install the VPN Concentrator, and configure the minimal parameters to make it operate (called Quick Configuration).

The *VPN 3000 Concentrator Series User Guide* provides details on all the functions available in the VPN Concentrator 3000 Manager, and guidelines for configuring the VPN Concentrator.

The VPN Concentrator Manager also includes extensive online help that a system administrator can access by clicking the **Help** icon on the toolbar in the Manager window.

This user guide, the *VPN 3000 Concentrator Series Getting Started* manual, the *VPN 3000 Concentrator Series User Guide*, and this *VPN 3000 Client User Guide* are provided on the Cisco VPN 3000 Concentrator's software distribution CD-ROM in PDF format. To view the latest version on the Cisco Web site, go to the following site and click onVPN Clients.

http://www.cisco.com/univercd/cc/td/doc/product/vpn/index.htm.

Other references

Other useful books, articles, and websites include:

Frequently Asked Questions about Microsoft VPN Security. Microsoft Corporation: 1998. (Available from Microsoft web site, `www.microsoft.com`.)

Kosiur, Dave. *Building and Managing Virtual Private Networks*. Wiley: 1998.

Sheldon, Tom. *Encyclopedia of Networking*. Osborne/McGraw-Hill: 1998.

Stallings, William. *Data and Computer Communications*, 5th ed. Prentice-Hall: 1997.

Virtual Private Networking: An Overview. Microsoft Corporation: 1999. (Available from Microsoft web site.)

`www.ietf.org` for Internet Engineering Task Force (IETF) Working Group drafts on IP Security Protocol (IPSec).

Documentation Conventions

We may use these typographic conventions in this manual:

Font	Meaning
This font	Document, chapter, and section titles. Emphasized text.
`This font`	Command-line prompts and entries, data-entry-field entries, system displays, filenames, etc.
`This font`	Literal entries you should make exactly as shown.
<This font>	Variables that the system supplies. Ignore the angle brackets.
This font	Menus, menu items, keyboard keys, icons, screen names, data-entry field names, etc.

Data Formats

As you configure and manage the VPN Client, enter data in these formats unless the instructions indicate otherwise.

IP addresses

IP addresses use 4-byte dotted decimal notation; for example, `192.168.12.34`. You can omit leading zeros in a byte position.

Hostnames

Hostnames use legitimate network host or end-system name notation; for example, `VPN01`. Spaces are not allowed. A hostname must uniquely identify a specific system on a network. A hostname can be up to 255 characters in length.

Usernames and Passwords

Text strings for usernames and passwords use alphanumeric characters, upper- and lower-case. Most text strings are case-sensitive; for example, `simon` and `Simon` represent different usernames. The maximum length of usernames and passwords is generally 32 characters.

Terminology

In this user guide, the term Cisco VPN device refers to the following Cisco products:

Cisco VPN 3000 Concentrator Series

Cisco VPN 5000 Concentrator Series

Cisco Secure PIX Firewall devices

IOS platform devices, such as the Cisco 7100 Series Routers

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

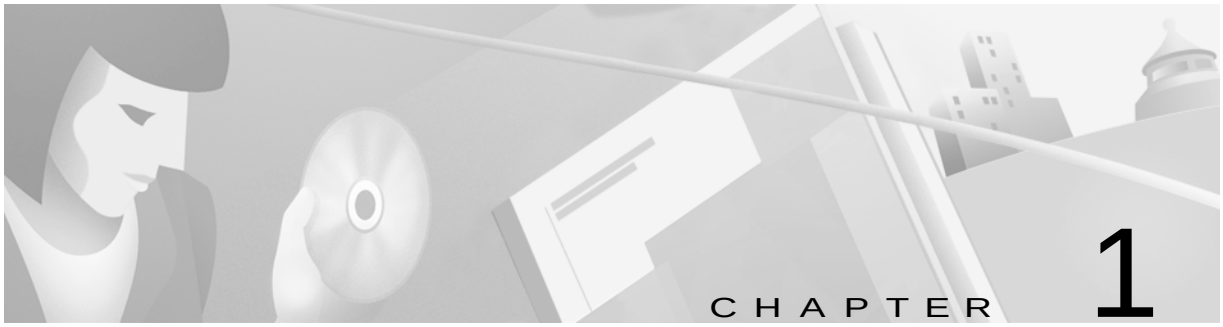
Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



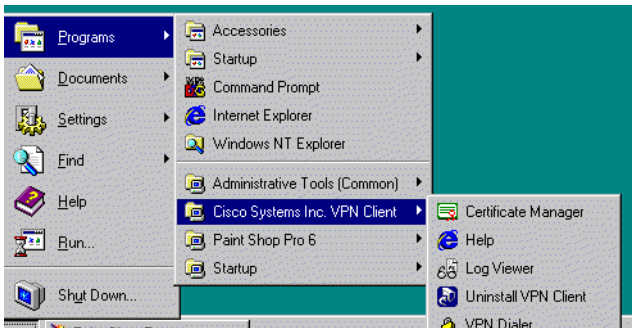
Understanding the VPN Client

The VPN Client is a software program that runs on a Microsoft® Windows®-based PC. The VPN Client on a remote PC, communicating with a Cisco VPN device at an enterprise or service provider, creates a secure connection over the Internet that lets you access a private network as if you were an on-site user. That's why it's called a VPN: a Virtual Private Network.

As a remote user (low speed or high speed), you first connect to the Internet. Then you use the VPN Client to securely access the private enterprise network through a Cisco VPN device that supports the VPN Client.

The VPN Client comprises the following applications, which you select from the Program menu:

Figure 1-1: VPN Client applications



In logical order of use, the applications are as follows:

- **Help** — displays an online manual with instructions on using the applications (Chapter 3, *Configuring the VPN Client*).
- **VPN Dialer** — lets you configure connections to a VPN device and lets you then start your connections (Chapter 3, *Configuring the VPN Client* and Chapter 4, *Connecting to a private network*).
- **Certificate Manager** — lets you enroll for certicates to authenticate your connections to VPN devices (Chapter 6, *Enrolling and managing certificates*).
- **Log Viewer** — lets you display events from the log (Chapter 5, *Managing the VPN Client*).
- **SetMTU** — lets you change the MTU setting on your PC, used for troubleshooting (Chapter 5, *Managing the VPN Client*).
- **Uninstall VPN Client** — lets you safely remove the VPN Client software from your system and retain your connection and certificate configurations (Chapter 5, *Managing the VPN Client*).

How it works

The VPN Client works with a Cisco VPN device to create a secure connection, called a tunnel, between your computer and the private network. It uses Internet Key Exchange (IKE) and Internet Protocol Security (IPSec) tunneling protocols to make and manage the secure connection. Some of the steps include:

- Negotiating tunnel parameters: addresses, algorithms, lifetime, etc.
- Establishing tunnels according to the parameters.
- Authenticating users: making sure users are who they say they are, via usernames, group names and passwords, and X.509 digital certificates.
- Establishing user access rights: hours of access, connection time, allowed destinations, allowed protocols, etc.
- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

For example, to use a remote PC to read email at your organization, you connect to the Internet, then start the VPN Client and establish a secure connection through the Internet to your organization's private network. When you open your email, the Cisco VPN device uses IPSec to encrypt the email message; and it transmits the message through the tunnel to your VPN Client, which decrypts the message so you can read it on your remote PC. If you reply to the email message, the VPN Client uses IPSec to process and return the message to the private network through the Cisco VPN device.

Connection technologies

The VPN Client lets you use any of the current technologies to connect to the Internet:

- POTS (Plain Old Telephone Service): uses a dial-up modem to connect.
- ISDN (Integrated Services Digital Network): may use a dial-up modem to connect.
- Cable: uses a cable modem; always connected.
- DSL (Digital Subscriber Line): uses a DSL modem; always connected.

You can also use the VPN Client on a PC with a direct LAN connection.

Features

- IPSec tunneling protocol.
- IKE key management protocol.
- IKE Keepalives — monitoring the continued presence of a peer and reporting the VPN Client's continued presence to the peer, which prevents hung connections due to loss of connectivity.
- Data compression for modem users, which speeds transmission.
- Split tunneling — the ability to simultaneously direct packets over the Internet in clear text and encrypted through an IPSec tunnel.
- User authentication via VPN Concentrator:
  - Internal VPN Concentrator server database.
  - RADIUS (Remote Authentication Dial-In User Service).
  - NT Domain (Windows NT®).

  - RSA (formerly SDI) SecurID or SoftID.
- Automatic connection via Microsoft Dial-Up Networking.
- Automatic VPN Client configuration option.
- Log Viewer — an application that collects events for viewing and analysis.
- Set MTU size — the ability to control the size of packets sent through the network.
- Certificate Manager — an application that lets you manage your identity certificates.
- Complete browser-based context-sensitive HTML Help.
- Support for Cisco Secure PIX Firewall platforms that run Release 6.0 and above.
- Support for VPN Concentrator Series 3000 platforms.
- LZS data compression.
- Command line interface to the VPN Dialer.
- Start Before Logon — the ability to establish a VPN connecton before logging on to a Windows NT or Windows 2000 system.
- Application Launcher — the ability to launch an application from the logon desktop.

Note: Instructions on configuring the VPN Client to interoperate with Cisco Secure PIX Firewall, Release 6.0, are available in *IPSec User Guide for Cisco Secure PIX Firewall.*

VPN Client IPSec attributes

The VPN Client supports these IPSec attributes:

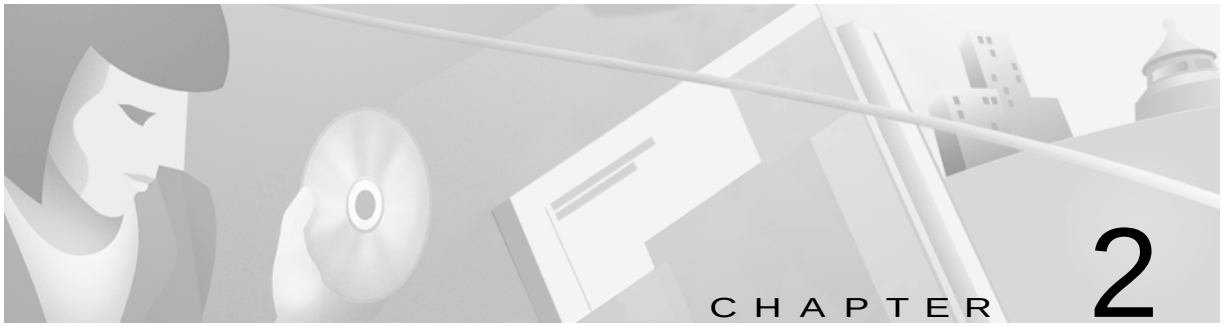
- Main mode for negotiating phase one of establishing ISAKMP Security Associations (SAs).
- Aggressive mode for negotiating phase one of establishing ISAKMP SAs.
- Authentication algorithms:
  - HMAC (Hashed Message Authentication Coding) with MD5 (Message Digest 5) hash function.
  - HMAC with SHA-1 (Secure Hash Algorithm) hash function.
- Authentication Modes:
  - Preshared Keys.
  - X.509 Digital Certificates.
- Diffie-Hellman Groups 1, 2, and 5.
- Encryption algorithms:
  - 56-bit DES (Data Encryption Standard).
  - 168-bit Triple-DES.
- Extended Authentication (XAUTH).
- Mode Configuration (also known as ISAKMP Configuration Method).
- Tunnel Encapsulation Mode.
- IP compression (IPCOMP) using LZS.

Getting started

To use the VPN Client, you must do only three things:

- Install it. (Chapter 2.)
- Configure it. (Chapter 3.)
- Connect to the private network with it. (Chapter 4.)

To begin, turn to Chapter 2, *Installing the VPN Client*.



Installing the VPN Client

This chapter explains how to install the VPN Client on your PC. The steps are:

- Verify that your computer meets the system requirements.
- Gather information you need.
- Install the VPN Client software.

To install a new version of the VPN Client, or to uninstall it, see Chapter 5.

Note: Installing the VPN Client software on Windows NT or Windows 2000 requires Administrator privileges. If you do not have Administrator privileges, you must have someone with Administrator privileges install the product for you.

Verifying system requirements

Verify that your computer meets these requirements:

- Computer with a Pentium®-class processor or greater.
- One of the following operating systems:
  - Microsoft® Windows® 95, Windows 98, or Windows 98 second edition
  - Windows ME
  - Windows NT® 4.0 (with Service Pack 3, or higher)
  - Windows 2000
- Microsoft TCP/IP installed. (Confirm via **Start > Settings > Control Panel > Network > Protocols** or **Configuration**.)
- 10 MB hard disk space.
- RAM:
  - 16 MB for Windows 95/98, or
  - 32 MB for Windows NT and Windows ME.
  - 64 MB for Windows 2000.

- *To install the VPN Client:*
  - CD-ROM drive, or
  - 3.5” high-density diskette drive, or
  - Network connection.
  - Administrator privileges if installing on Windows NT or Windows 2000.
- *To use the VPN Client:*
  - Direct network connection (cable or DSL modem and network adapter/interface card), or
  - Internal or external modem, *and*
  - For Windows 95, Microsoft Dial-Up Networking (DUN) version 1.2 or greater. (DUN 1.3 for Windows 95 is a recommended performance and security upgrade, and it is available as a free download from the Microsoft Web site, `www.microsoft.com`. Windows 98 includes the DUN 1.3 functionality.)
- *To connect using a digital certificate for authentication:*
  - A digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC.

    Baltimore Technologies (www.baltimoretechnologies.com).

    Entrust Technologies (www.entrust.com).

    GTE Cybertrust (www.cybertrust.com).

    Verisign, Inc. (www.verisign.com).

    Microsoft Certificate Services — Windows 2000.

Gathering information you need

To configure and use the VPN Client, you may need the information listed in Table 2-1.

Ask for this information from the system administrator of the private network you want to access. Your system administrator may have preconfigured much of this data; if so, he or she will tell you which items you need.

We suggest you record the data now and refer to it as you proceed. *To protect security, we suggest you memorize, rather than write, passwords, PIN, etc.*

Table 2-1: VPN Client information worksheet

Information you may need	Write your data here
Hostname or IP address of the remote device to which you are connecting.	
Your IPSec Group Name (pre-shared keys).	
Your IPSec Group Password (pre-shared keys).	
If you connect via an ISP (Internet Service Provider), your logon username [and password].	

Table 2-1: VPN Client information worksheet (continued)

Information you may need	Write your data here
If you are using a certificate for authentication, the name of your certificate.	
If you are authenticated via the VPN Concentrator internal server, your username [and password].	
If you are authenticated via a RADIUS server, your username [and password].	
If you are authenticated via an NT Domain server, your username, [password,] and domain name.	
If you are authenticated via SecurID or SoftID, your username [and PIN].	
If you should configure backup server connections, the hostnames or IP addresses of the backup servers.	
If you connect to the ISP via Dial-Up Networking: • Phone number of the ISP. • Modem properties. • Server types. • Protocols. • TCP/IP settings. • Scripting. • Multilink settings.	

Installing the VPN Client

To install the VPN Client on your system, follow these steps. We suggest you accept the defaults unless your system administrator has instructed otherwise.

1. Exit all Windows programs, and disable any anti-virus software.
2. Start the appropriate VPN Client installation setup program:

•If VPN Client software is on CD-ROM:

a. Insert the Cisco Systems CD-ROM in your system's CD-ROM drive.
b. Select **Start** > **Run**. The **Run** dialog box appears.
c. Enter `E:\VPN Client\CD-ROM\setup`, where `E:` is your system's CD-ROM drive.
d. Click **OK**.

•If VPN Client software is on diskettes:

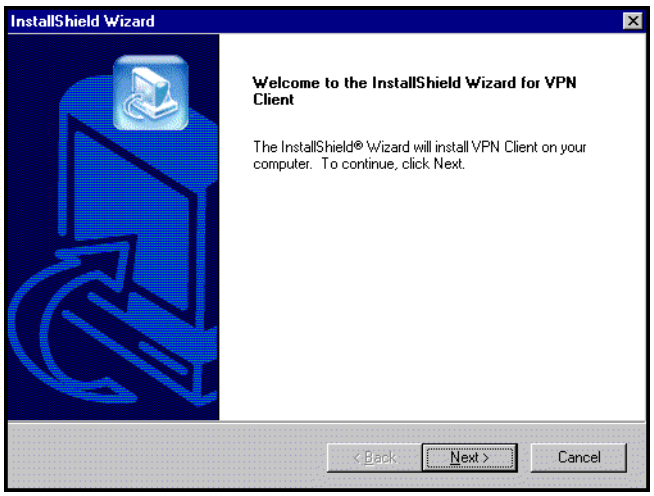
a. Insert Disk 1 (of three) in your system's diskette drive.
b. Select **Start** > **Run**. The **Run** dialog box appears.
c. Enter `A:\setup`, where `A:` is your system's diskette drive.
d. Click **OK**.

•If VPN Client software is on a network:

a. Use Explorer to open the folder or directory containing the VPN Client software.
b. Locate the file `Setup.exe`.
c. Double click `Setup.exe`.

The program displays the Cisco Systems logo and InstallShield Setup window (Figure 2-1).

Figure 2-1: Initial VPN Client installation window

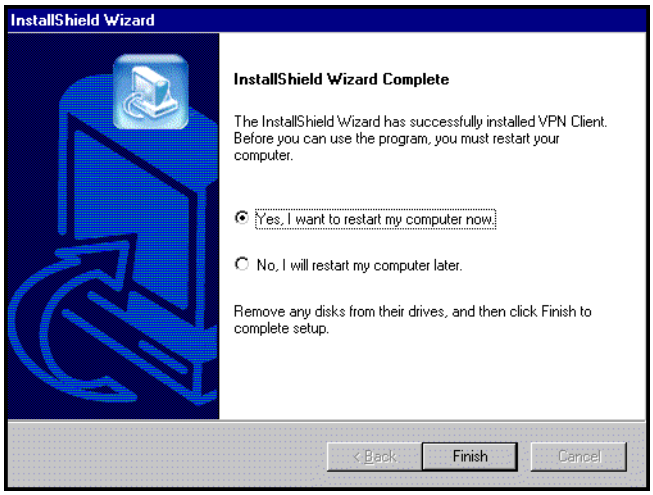

InstallShield Wizard
Welcome to the InstallShield Wizard for VPN Client
The InstallShield® Wizard will install VPN Client on your computer. To continue, click Next.
< Back
Next >
Cancel

Follow the directions on the screens and enter the following information:

A destination folder for the VPN Client files (or **Next>** to enter the default location `C:\Program Files\Cisco Systems\VPN Client`).

After you have installed the VPN Client, the InstallShield Wizard displays the following screen. You must restart your computer before you can configure and use the VPN Client (Figure 2-2).

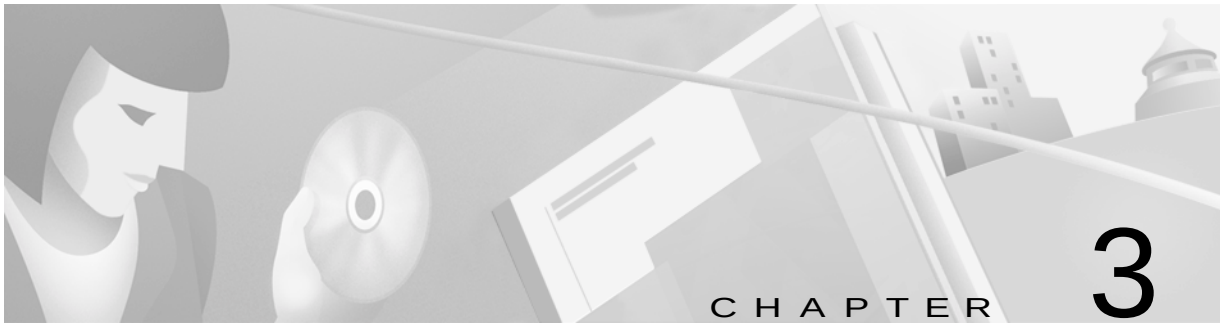
Figure 2-2: Setup Complete dialog box


InstallShield Wizard
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed VPN Client. Before you can use the program, you must restart your computer.
Yes, I want to restart my computer now.
No, I will restart my computer later.
Remove any disks from their drives, and then click Finish to complete setup.
< Back
Finish
Cancel

– To restart now, click **Finish**. Your system reboots. *Be sure to remove any diskette from the drive before you reboot.*
– To restart later, click the **No** radio button and then click **Finish**. The VPN Client Setup closes. Remember: *you must restart your computer before you can use the VPN Client.*

What next?

The VPN Client software is now installed on your PC. Next you must configure it. To proceed, turn to Chapter 3, *Configuring the VPN Client*.



Configuring the VPN Client

This chapter explains how to configure the VPN Client.

To configure the VPN Client, you enter values for a set of parameters known as a *connection entry.* The VPN Client uses a connection entry to identify and connect securely to a specific private network.

Parameters include a name and description for the connection, the name or address of the VPN device (the remote server), and information that identifies you to the VPN device.

Note: If your system administrator has completely preconfigured your connection entry, you can skip this chapter and go directly to Chapter 4, *Connecting to a private network*.

The rest of this chapter explains how to

- Create a new connection entry.
- Set or change connection entry properties:
  - General:

    Connection entry description.

    Allow IPSec through NAT.

    Peer response timeout.

    Logon to Microsoft Network (for Windows 95, Windows 98, and Windows ME only).
  - Authentication:

    For using preshared keys — IPSec group name and password.

    For certificate — Name of certificate.
  - Connections:

    Enable or remove backup servers.

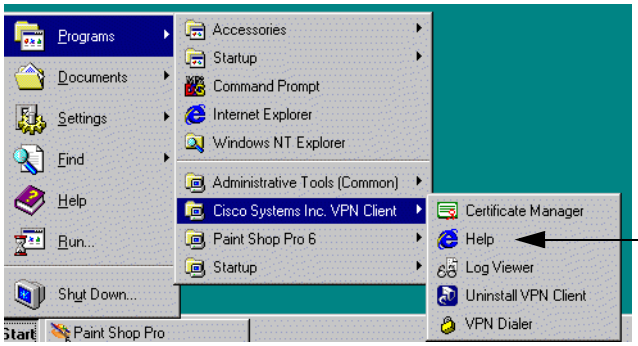
    Connect via Dial-Up Networking.
- Change remote server address for a connection entry.

How to get help

The VPN Client comes with a complete, context-sensitive HTML help system. You can display help in the following ways:

- On the Program Menu, select **Start > Programs > Cisco Systems VPN Client > Help (**Figure 3-1**)**.

Figure 3-1: Cisco Systems VPN Client program menu



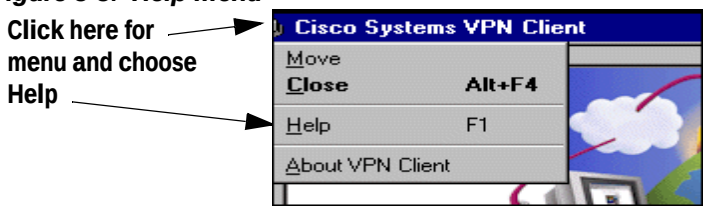
- Press F1 at any window while using the VPN Client.
- Select the Help button, on windows that display it (Figure 3-2).

Figure 3-2: Help button

New Connection Entry Wizard
Cisco Systems
Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries.
Group Access Information
Name:
Password:
Confirm Password:
Certificate
Name:
No Certificates Installed
Validate Certificate...
< Back
Next >
Cancel
Help
Help button

- Select **Help** from the menu that appears when you click on the icon in the title bar (Figure 3-3).

Figure 3-3: Help menu



Determining the VPN Client version

To display the version number of the software release you are currently using, follow these steps:

1. Click the icon in the title bar (Figure 3-3).

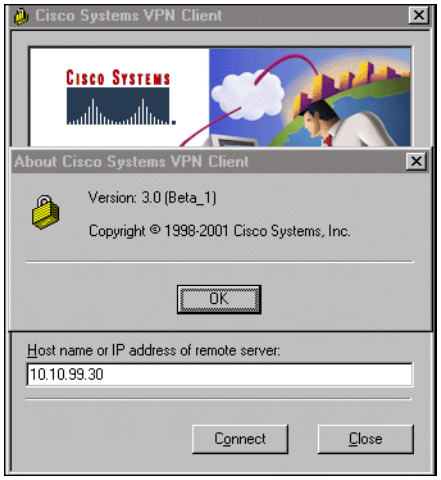
   The VPN Client displays a menu.

2. Click **About VPN Client** on the menu displayed.

   The VPN Client that displays the version you are currently using (Figure 3-4).

3. After viewing the version number, click **OK**.

Figure 3-4: Displaying the VPN Client software version



What is a connection entry?

To use the VPN Client, you must create at least one connection entry, which identifies:

- The VPN device (the remote server) to access.
- For preshared keys — The IPSec group to which the system administrator assigned you. Your group determines how you access and use the remote network. For example, it specifies access hours, number of simultaneous logins, user authentication method, and the IPSec algorithms your VPN Client uses.
- For certificates — The name of the certificate you are using for authentication.
- Optional parameters that govern VPN Client operation and connection to the remote network.

You can create multiple connection entries if you use your VPN Client to connect to multiple networks (though not simultaneously), or if you are a member of more than one of the groups defined for a VPN device.

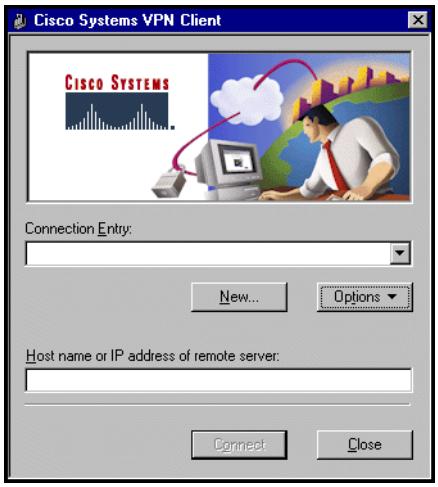
Reminder: Refer to Table 2-1, “VPN Client information worksheet,” on page 2-2 for connection entry parameters.

How to create a new connection entry

Start the VPN Client by selecting **Start > Programs > Cisco Systems VPN Client > VPN Dialer**.

The VPN Client starts and displays its main dialog (Figure 3-5).

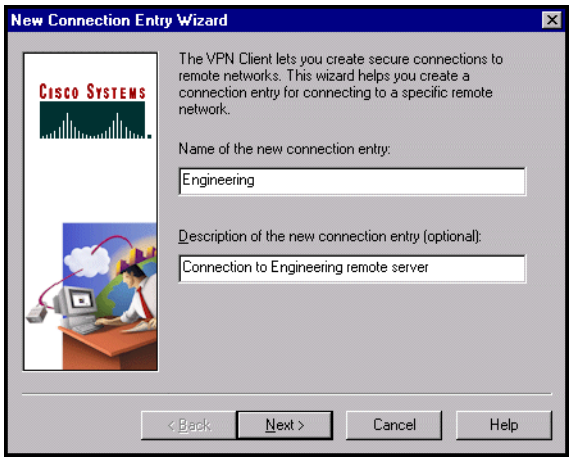
Figure 3-5: VPN Client main dialog



1 At the main dialog, click **New**.

The first **New Connection Entry Wizard** dialog appears (Figure 3-6).

Figure 3-6: New Connection Entry Wizard dialog


New Connection Entry Wizard
Cisco Systems
The VPN Client lets you create secure connections to remote networks. This wizard helps you create a connection entry for connecting to a specific remote network.
Name of the new connection entry:
Engineering
Description of the new connection entry (optional):
Connection to Engineering remote server
< Back
Next >
Cancel
Help

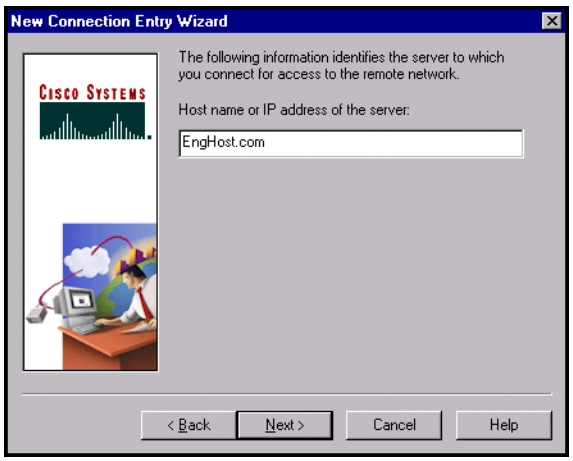
2 Enter a unique name for this new connection. You can use any name to identify this connection; for example, *Engineering*. This name can contain spaces, and it is not case-sensitive.

3 Enter a description of this connection. This field is optional, but it helps further identify this connection. For example, *Connection to Engineering remote server.*

4 Click **Next**.

The second **New Connection Entry Wizard** dialog appears (Figure 3-7).

Figure 3-7: New Connection Entry Wizard dialog 2


New Connection Entry Wizard
Cisco Systems
The following information identifies the server to which you connect for access to the remote network.
Host name or IP address of the server:
EngHost.com
< Back
Next >
Cancel
Help

5 Enter the hostname or IP address of the remote VPN device you want to access, and click **Next**.

The third **New Connection Entry Wizard** dialog appears (Figure 3-8).

6 You can connect as part of a group or via an identity digital certificate.

Figure 3-8: New Connection Entry Wizard dialog 3

New Connection Entry Wizard
Cisco Systems
Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries .
Group Access Information
Name:
Password:
Confirm Password:
Certificate
Name:
No Certificates Installed
Validate Certificate...
< Back
Next >
Cancel
Help

- *If you are using group authentication* --
  - Enter the following information in the dialog (Figure 3-9):
  - In the **Name**: field, enter the name of the IPSec group to which you belong– Maximum 32 characters. This entry is case-sensitive.
  - In the **Password**: field, enter the password (also case-sensitive) for your IPSec group – Maximum 32 characters. The field displays only asterisks.
  - Verify your password by entering it again in the **Confirm Password** field.

Figure 3-9: (Group)

New Connection Entry Wizard
Cisco Systems
Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries .
Group Access Information
Name:
RemoteUsers
Password:
Confirm Password:
Certificate
Name:
No Certificates Installed
Validate Certificate...
< Back
Next >
Cancel
Help

- *If you are using certificate authentication* (Figure 3-10) --

  – Select the name of the certificate you are using. If the field says **No Certificates Installed** and is shaded, then you must first install a certificate before you can use this feature. For information on enrolling fora certificate, see Chapter 6, .

***Figure 3-10:* (Certificate)**

New Connection Entry Wizard
Cisco Systems
Your administrator may have provided you with group parameters or a digital certificate to authenticate your access to the remote server. If so, select the appropriate authentication method and complete your entries .
Group Access Information
Name:
Password:
Confirm Password:
Certificate
Name:
Patrick Clarkson (Microsoft)
Validate Certificate...
< Back
Next >
Cancel
Help

  – To verify the validity of the certificate, click **Validate Certificate...** and enter the password. You'll receive a report letting you know whether the password is valid. If not, you need to try again. If you don't know or can't remember the password, see your system administrator. An identity certificate has a public and private key, and a time period within which it is valid. Make sure the certificate is valid before you continue.

  – After you have verified that the certificate has a valid password, click **Next**.

The fourth **New Connection Entry Wizard** dialog appears (Figure 3-11).

Figure 3-11: New Connection Entry Wizard dialog 4

New Connection Entry Wizard
Cisco Systems
You have successfully created a new virtual private networking connection entry named:
Engineering
Click Finish to save this entry.
To connect to the remote network, select the Dial button from the main window.
To modify this connection entry, click Options on the main window and select Properties from the menu that appears.
< Back
Finish
Cancel
Help

7 Review the connection entry name. If you want to change any previous entries, click **Back** until you get to the desired dialog.

8 To complete your entry, click **Finish**.

The **New Connection Entry Wizard** dialog closes. Your new connection entry now appears in the **Connection Entry** drop-down list on the VPN Client's main dialog.

What next?

If you need to configure optional connection entry parameters, or change parameters for an existing connection entry, continue to the next section.

Otherwise, you can skip to Chapter 4, *Connecting to a private network.*

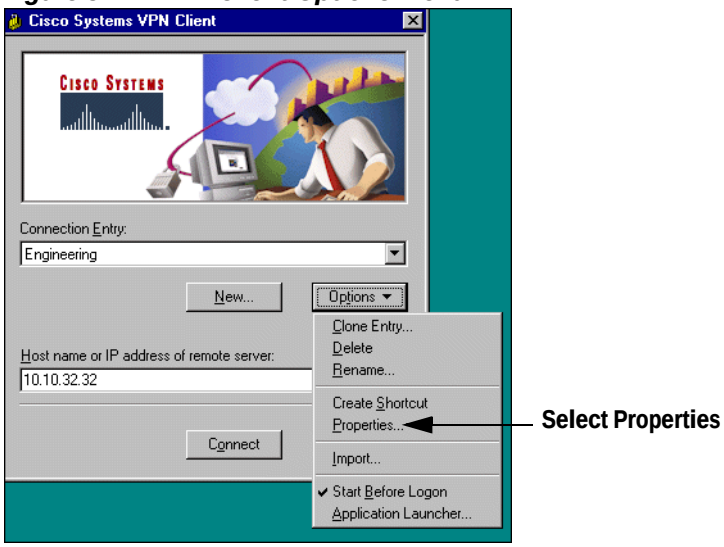
Setting or changing connection entry properties

To change parameters or to set optional parameters for an existing connection entry:

1 On the VPN Client's main dialog, click the **Connection Entry** drop-down menu button and select the entry you want to configure.

2 Then click **Options** and select **Properties** from the menu (Figure 3-12).

Figure 3-12: VPN Client Options menu



The **Properties** dialog appears.

The fields in this dialog differ according to the operating system you are using.

- If you are using Microsoft Windows 95 or Windows 98, you see the dialog that looks like the one in Figure 3-13.
- If you are using Microsoft Windows NT or Windows 2000, you see the dialog in Figure 3-14.

Figure 3-13: Connection Entry Properties dialog (Windows 95 and Windows 98)

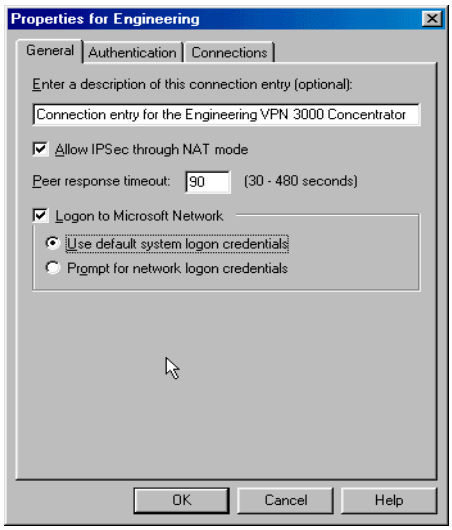
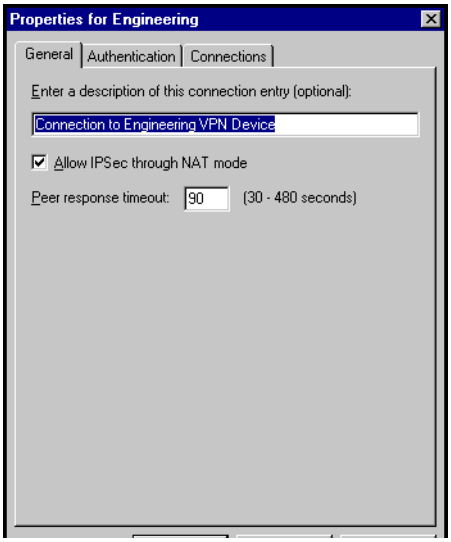


Figure 3-14: Connection Entry Properties dialog (Windows NT and Windows 2000)



3 Click the tab for the parameters you want to change:

- **General** tab
  - Changing the connection entry description.
  - Allow IPsec through NAT mode.
  - Peer response timeout in seconds
  - Logging on to Microsoft Network (Windows 95/98).
- **Authentication** tab
  - Changing the group name or group password.
  - Changing the certificate you want to use.
- **Connections** tab
  - Enabling, adding, and removing backup server connections.
  - Connecting to the Internet via Dial-Up Networking.

See the appropriate section of this chapter for each tab and parameter.

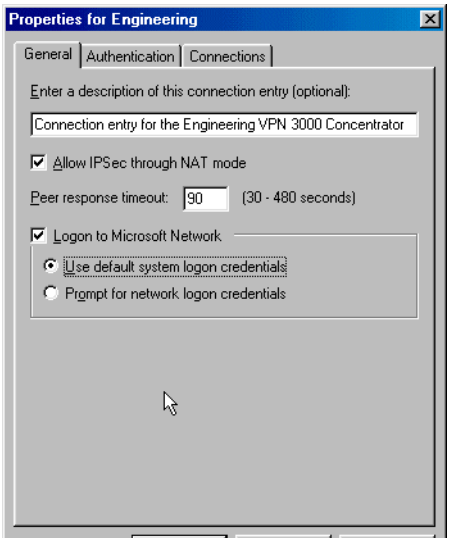
4 When you are finished setting parameters, click **OK**. The **Properties** dialog closes and saves your changes.

To discard your changes, click **Cancel**. The **Properties** dialog closes and discards all changes.

Changing General settings

The **Properties > General** tab lets you set general parameters for this connection entry (Figure 3-15).

Figure 3-15: Properties dialog > General tab



Changing connection entry description

To change the description of this connection entry, enter or edit the description field. This field is optional, and it's to help you identify this connection.

Allowing IPSec through NAT mode

Allow IPSec through NAT mode enables secure transmission between the client and the VPN device through a router serving as a firewall, which may also be performing Network Address Translation (NAT) or Port Address Translations (PAT).

The most common application for IPSec through NAT mode is behind a home router performing PAT. Using this feature encapsulates Protocol 50 (ESP) traffic within UDP packets that the home router forwards to their destination. The VPN Client also sends keepalives frequently, ensuring that the mappings on the router are kept active.

Not all routers support multiple simultaneous connections behind them. Some routers can't map additional sessions to unique source ports. Therefore, it's important to check with your router vendor to verify whether this limitation exists. Some router vendors support Protocol-50 (ESP) Port Address Translation, which may let you operate without using IPSec through NAT mode.

To use IPSec through NAT, the central-site group in the Cisco VPN device must be configured to support it. For an example, refer to the VPN Concentrator Manager, **Configuration | User Management | Groups | IPSec** tab (see *VPN 3000 Concentrator Series User Guide* or refer to the VPN Concentrator Manager Help).

This parameter is enabled by default. To disable this parameter, clear the check. We recommend that you always keep this parameter checked.

Adjusting the peer response timeout

The VPN Client uses a keepalive mechanism called Dead Peer Detection (DPD) to detect if the VPN device on the other side of an IPSec tunnel is unavailable. If the network is unusually busy or unreliable, you may need to increase the number of seconds to wait before the VPN Client decides that the peer is no longer active. The default number of seconds to wait before terminating a connection is 90 seconds. The minimum number of seconds you can configure is 30 seconds and the maximum is 480 seconds.

To adjust the setting, enter the number of seconds in the **Peer response timeout** field.

The VPN Client continues to send DPD requests every 5 seconds, until it reaches the number of seconds specified by the **Peer response timeout** value.

Logging on to Microsoft Network (Windows 95, Windows 98, and Windows ME)

The **Logon to Microsoft Network** parameter registers your PC on the private Microsoft network and lets you browse and use network resources after the VPN Client establishes a secure connection. This parameter is enabled by default.

To disable this parameter, clear the check.

Note: This parameter appears only on VPN Clients installed on systems running Windows 95, Windows 98, and Windows ME. For information on logging on to Windows NT and Windows 2000 systems, see "Starting connections before logging on (Windows NT and Windows 2000 only)" in Chapter 5.

If you do not need or do not have privileges for Microsoft Windows resources on the private network, disable this parameter. For example, if you require only FTP access to the private network, you could disable this parameter.

If you enable this parameter, click one of the radio buttons to select the logon process:

Use default system logon credentials = Use the Windows logon username and password on your PC to log on to the private network. With this option, you do not need to manually enter your logon username and password each time you connect to the private network. This is the default selection.

Prompt for network logon credentials = The private network prompts you for a username and password to use its resources. If the logon username or password on your PC differs from those on the private network, use this option.

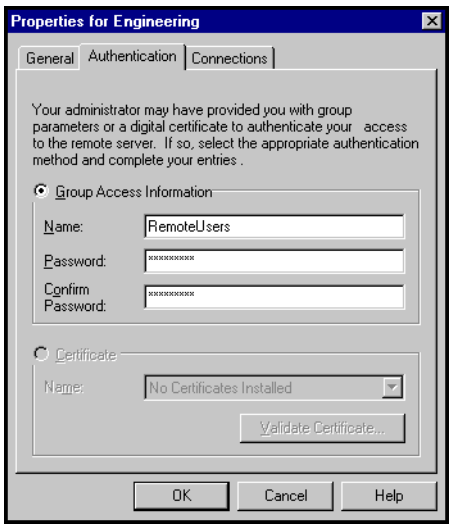
When you are done with the General tab, click **OK** or click another tab.

Changing Authentication settings

The **Properties > Authentication** tab (Figure 3-16) lets you change the name or password of the IPSec group to which you are assigned. Your group determines your access to, and use of, the remote network. The group name and password are essential parameters in authenticating you as a user of the remote network.

If you want to choose a different certificate, you also use this screen.

Figure 3-16: Properties dialog > Authentication tab



Changing group name or group password

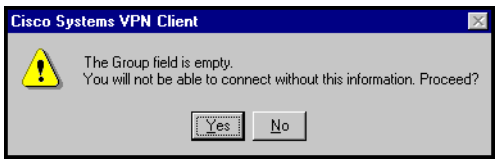
You usually specify a group name and group password when you create a connection entry. However, you can use the Authentication tab to change a group name or group password if your system administrator so instructs you; or to enter the group name and password if the connection entry does not already have them.

In the **Name** field, enter or edit the group name – maximum 32 characters. This entry is case-sensitive.

In the **Password** field, enter or edit the group password – maximum 32 characters. This entry is case-sensitive. The field displays only asterisks. Verify your password by entering it again in the **Confirm Password** field.

If either field is empty when you leave this dailog, the VPN Client reminds you to enter missing group information (Figure 3-17). To proceed, click **Yes**, or to terminate, click **No**.

Figure 3-17: Reminder dialog

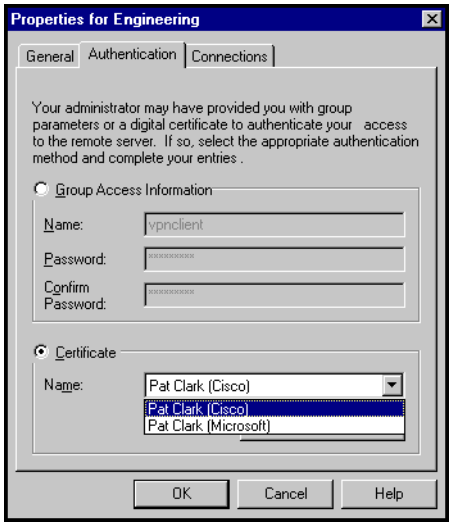

Cisco Systems VPN Client
The Group field is empty.
You will not be able to connect without this information. Proceed?
Yes
No

When you are done with the Authentication tab, click **OK** or click another tab.

Selecting a different certificate

To select a different certificate, make sure the radio button for **Certificate** is selected, then click the drop down menu of certificates installed on your PC and select one (Figure 3-18).

Figure 3-18: Selecting a certificate

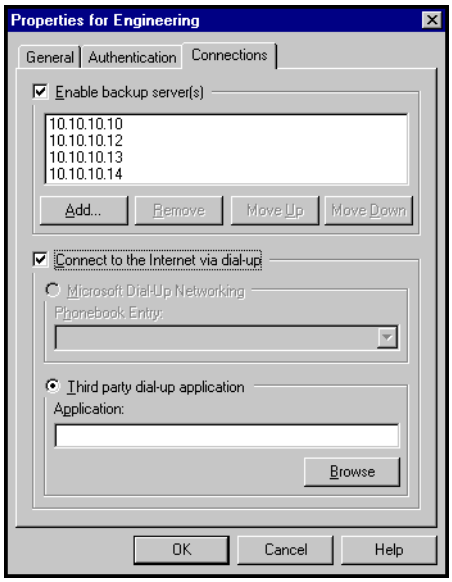


When you are done with the Authentication tab, click **OK** or click another tab.

Changing Connection settings

The **Properties > Connections** tab (Figure 3-19) lets you set parameters that govern how you connect to the private network. You can enable and configure backup server connections, and automatically launch a dial-up networking application to connect to the Internet.

Figure 3-19: Properties dialog > Connections tab



Enabling and adding backup servers

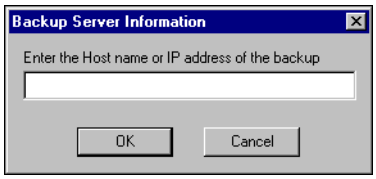
The private network may include one or more backup VPN devices (servers) to use if the primary server is not available. Your system administrator tells you whether to enable a backup server and gives you its address. Refer to your entries in Table 2-1, "VPN Client information worksheet," on page 2-2.

1 To enable backup servers, check the **Enable backup server(s)**. This is not checked by default.

2 You can now click **Add** to enter its address.

The **Backup Server Information** dialog appears (Figure 3-20).

Figure 3-20: Backup server information dialog



3 Enter the hostname or IP address of the backup server – maximum 255 characters.

4 Click **OK**.

The hostname or IP address appears in the **Enable backup server(s)** list (Figure 3-19).

5 To add more backup devices, repeat Steps 2, 3, and 4.

Removing backup servers

To remove a server from the backup list, select the server from the list and click **Remove**. *There is no confirmation or undo.* The server name no longer appears in the list.

Changing the order of the servers

To reorder the servers in the list, select a server and click **Move Up** to increase the server's priority or **Move Down** to decrease the server's priority.

Disabling backup servers

You can disable using backup servers without removing backup servers from the list.

To disable using backup servers, clear the **Enable backup server(s)** check.

Configuring a connection to the Internet via dial-up networking

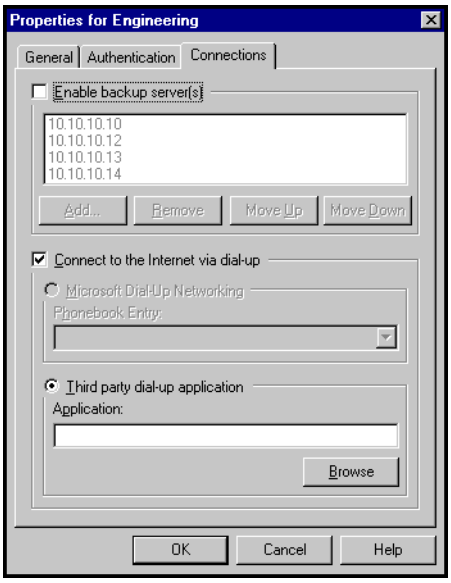
Connecting to a private network using a dial-up connection is typically a two-step process:

1 Use a dial-up connection to your Internet service provider (ISP) to connect to the Internet.

2 Use the VPN Client to connect to the private network through the Internet.

To enable and configure this feature, check the **Connect to the Internet via dial-up**. This is not checked by default (Figure 3-21).

Figure 3-21: Connect to the Internet via dial-up



You can connect to the Internet using the VPN Dialer application in two different ways:

- Microsoft Dial-up Networking (DUN)
- Third party dial-up program

Microsoft Dial-up Networking

If you have DUN phonebook entries and **Connect to the Internet via dial-up** is enabled, Microsoft Dial-up Networking is enabled by default. To link a VPN Client connection entry to a Dial-Up Networking phonebook entry, do the following:

1. Click **Microsoft Dial-up Networking** (if it is not already enabled).
2. To link your VPN Client connection entry to a DUN entry, click the down arrow next to the **Phonebook entry** field and select an entry from the drop-down menu.

   The VPN Client then uses this DUN entry to automatically dial into the Microsoft network before making the VPN connection to the private network.

Third party dial-up program

If you have no DUN phonebook entries and **Connect to the Internet via dial-up** is enabled, then **Third party dial-up application** is enabled by default.

To connect to the Internet using a third party dial-up program, use the following procedure:

1. Click **Third party dial-up application**, if it is not already enabled.
2. Use **Browse** to enter the name of the program in the **Application** field. This application launches the connection to the Internet.

   This string you select or enter here is the pathname to the command that starts the application and the name of the command; for example: `c:\isp\ispdialer.exe dialEngineering`. Your network administrator may have set this up for you. If not and if you don't know the name of the program, consult your network administrator.

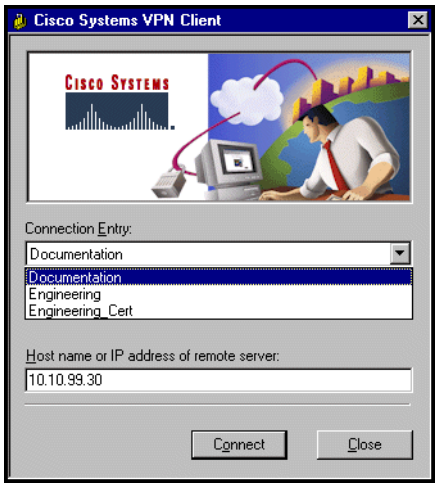
Changing the VPN device address for a connection entry

You can change the address of the VPN device in a connection entry, and you can make the change temporary or permanent.

1 Start the VPN Client. The **VPN Client** main dialog appears (Figure 3-22).

2 Click the **Connection Entry** drop-down menu button and select the entry, if it is not already displayed.

Figure 3-22: VPN Client main dialog



3 Edit the address in the **Host name or IP address of remote server** field.

4 Click **Connect**. The VPN Client displays a confirmation dialog (Figure 3-23).

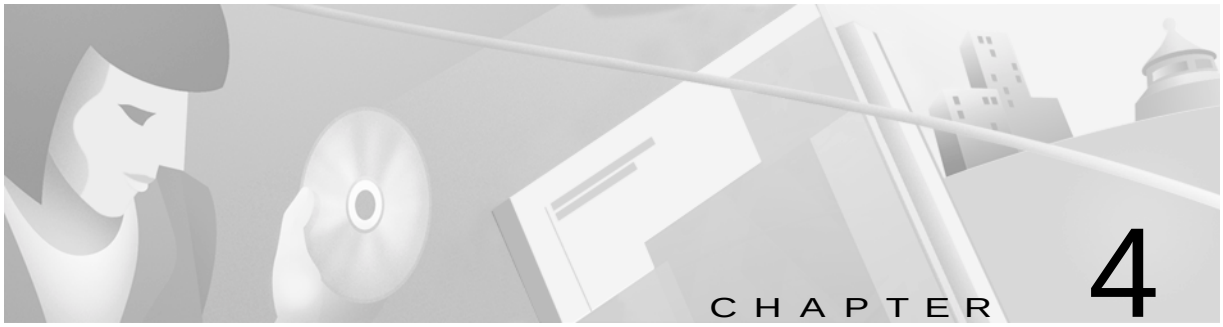
Figure 3-23: Address change dialog

5 Click one of the following:

To use this address for the current session only, click **No**. The VPN Client begins connecting to the VPN device, but it does not save your change with the connection entry.

To permanently change the address for this connection entry, click **Yes**. The VPN Client begins connecting to the VPN device, and it saves the new address with the connection entry.

For an explanation of the connection process, see Chapter 4.



Connecting to a private network

This chapter explains how to connect to a private network with the VPN Client.

We assume you have configured at least one VPN Client connection entry; as described in Chapter 3. To complete the steps in this chapter, you also need:

- ISP logon username and password, if necessary.
- User authentication information:
  - *If you are authenticated via the VPN Concentrator internal server,* your username and password.
  - *If you are authenticated via a RADIUS server,* your username and password.
  - *If you are authenticated via an Windows NT Domain server,* your username, password, and domain name.
  - *If you are authenticated via RSA Data Security (formerly SDI) SecurID or SoftID,* your username and PIN.
  - *If you use a digital certificate for authentication,* the name of the certificate, your username and password. If your private key is password protected for security reasons, you also need this password.

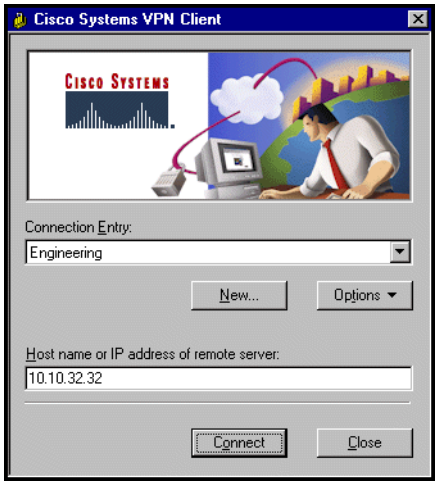
Reminder: Refer to your entries in Table 2-1, "VPN Client information worksheet," on page 2-2, as you complete steps here.

Starting the VPN Client

1 Start the VPN Client by selecting **Start > Programs > Cisco Systems VPN Client > VPN Dialer**.

The VPN Client displays its main dialog (Figure 4-1).

Figure 4-1: VPN Client main dialog



2 If necessary, click the **Connection Entry** drop-down menu button and select the desired connection entry.

Connection procedure

Connecting to a private network is a simple one- or two-step process:

1 Connect to the Internet, if necessary.

2 Connect to the private network through the Internet.

- Systems with cable or DSL modems are usually connected to the Internet, so no additional action is necessary. Skip to *Authenticating to connect to the private network*.
- Systems with modems or ISDN modems must connect to the Internet via Dial-Up Networking:
  - If you connect to the Internet via Dial-up Networking, proceed to *Using the VPN Client to connect to the Internet via Dial-Up Networking*.
  - If you must manually connect to the Internet, do it now. When your connection is established, skip to *Authenticating to connect to the private network*.
  - If your system is already connected to the Internet via Dial-Up Networking, skip to *Authenticating to connect to the private network*.

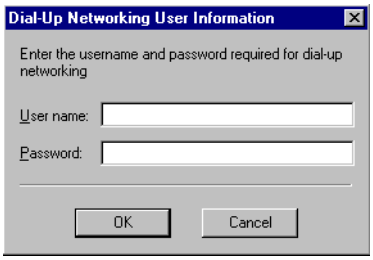
Using the VPN Client to connect to the Internet via Dial-Up Networking

This section describes how to connect to the Internet via Dial-Up Networking by running only the VPN Client. Your connection entry must be configured with **Connect to the Internet via Dial-Up Networking** enabled; see Chapter 3.

1 Click **Connect** on the VPN Client's main dialog (see Figure 4-1).

A **Dial-up Networking User Information** dialog appears (Figure 4-2). This dialog varies depending on the version of Windows you are using.

Figure 4-2: Dial-Up Networking User Information dialog

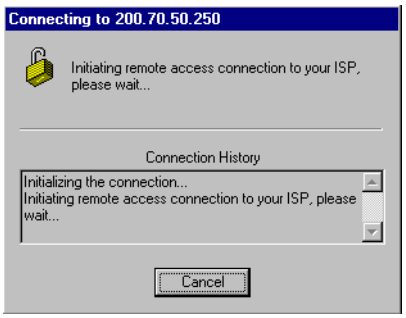


2 Enter the username and password to access your ISP. These entries may be case-sensitive. The **Password** field displays only asterisks.

3 Click **OK**.

You see the connection history dialog (Figure 4-3).

Figure 4-3: Confirming connections to ISP


Connecting to 200.70.50.250
Initiating remote access connection to your ISP, please wait...
Connection History
Initializing the connection...
Initiating remote access connection to your ISP, please wait...
Cancel

When the ISP connection is established, a Dial-Up Networking icon appears (Figure 4-4) in the system tray on the Windows taskbar.

Figure 4-4: Dial-Up Networking taskbar icon

Continue with the next section.

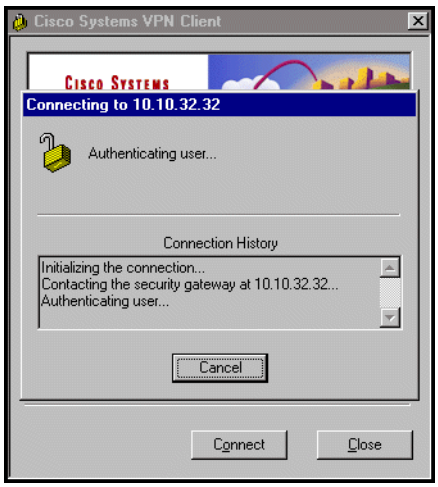
Authenticating to connect to the private network

This section assumes you are connected to the Internet. If you connect using Dial-Up Networking, verify that its icon is visible in the Windows taskbar system tray (Figure 4-4). If not, your Dial-Up Networking connection is not active and you need to establish it before continuing.

If you did not do so earlier, click **Connect** on the VPN Client's main dialog (Figure 4-1).

The VPN Client starts tunnel negotiation and displays a dialog (Figure 4-5).

Figure 4-5: Negotiating dialog



The next phase in tunnel negotiation is user authentication.

User authentication

User authentication means proving that you are a valid user of this private network. User authentication is optional. Your administrator determines whether it's required.

The VPN Client displays a user authentication dialog that differs according to the authentication method used by the IPSec group to which you are assigned. Your system administrator tells you which method you use.

Reminder: To continue, refer to your entries in Table 2-1 on page 2-2 and go to the appropriate section below.

Authenticating via the VPN device internal server or RADIUS server

The VPN Client displays the user authentication dialog. The title bar identifies the connection entry name.

Figure 4-6: Internal or RADIUS server authentication dialog

1. In the **Username** field, enter your username. This entry is case-sensitive.
2. In the **Password** field, enter your password. This entry is case-sensitive. The field displays only asterisks.
3. Click **OK**.

Note: If you cannot select the **Save Password** option, your administrator does not allow this option. If you can select this option, be aware that using it may compromise system security, since your password is then stored on your PC and is available to anyone who uses your VPN Client.

Skip to *Completing the private network connection*.

Authenticating via Windows NT Domain

The VPN Client displays the Windows NT Domain user authentication dialog. The title bar identifies the connection entry name.

Figure 4-7: Windows NT Domain authentication dialog

1. In the **Username** field, enter your username. This entry is case-sensitive.
2. In the **Password** field, enter your password. This entry is case-sensitive. The field displays only asterisks.
3. In the **Domain** field, enter your Windows NT Domain name, if it is not already there.
4. Click **OK**.

Skip to *Completing the private network connection*.

Authenticating via RSA Data Security (RSA) SecurID

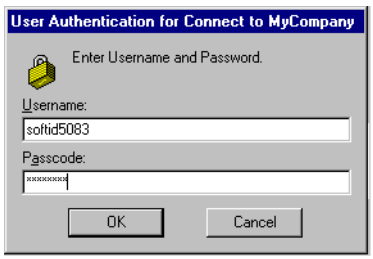
RSA (formerly SDI) SecurID authentication methods include physical SecurID cards and keychain fobs, and PC software called SoftID. SecurID cards also vary: with some cards, the passcode is a combination of a PIN and a cardcode; with others, you enter a PIN on the card and it displays a passcode. Ask your system administrator for the correct procedure.

Authentication via these methods also varies slightly for different operating systems. If you use an RSA method, the VPN Client displays the appropriate RSA user authentication dialog. The title bar identifies the connection entry name.

RSA User Authentication: SecurID Tokencards (Tokencards, Pinpads, and Keyfobs) and SoftID v1.0 (Windows 95 and Windows 98)

The VPN Client displays an authentication dialog asking for your username and passcode (Figure 4-8). If you are using SoftID, it must be running on your PC.

Figure 4-8: RSA authentication dialog



1. In the **Username** field, enter your username. This entry is case-sensitive.
2. In the **Passcode** field, enter an appropriate SecurID code. With SoftID, you can copy this code from the SoftID window and paste it here. Your administrator will tell you what you need to enter here, depending on the type of tokencard you are using.
3. Click **OK**.

RSA User Authentication: SoftID v1.x (Windows NT only) and SoftID v2.0 (all operating systems)

If you are using SoftID under Windows NT, the VPN Client displays an authentication dialog asking for your username and PIN.

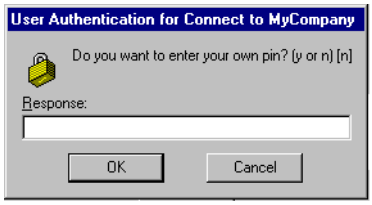
Figure 4-9: SoftID (Windows NT) authentication dialog

1. In the **Username** field, enter your username. This entry is case-sensitive.
2. In the **Pin** field, enter your SoftID PIN. The VPN Client gets the passcode directly from SoftID by communicating directly with SoftID. The SoftID application must be installed bud does not have to be running on your PC.
3. Click **OK**.

RSA New PIN Mode

The first time you authenticate using SecurID or SoftID (all operating systems), or if you are using a new SecurID card, and if the RSA administrator allows you to create your own PIN, the authentication program asks if you want to create your own PIN (Figure 4-10).

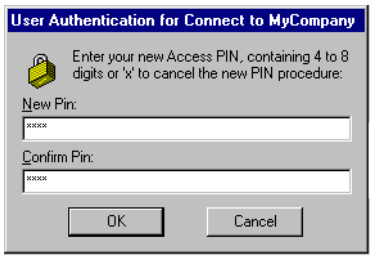
Figure 4-10: SecurID New PIN request



1 Enter your response **y** for yes or **n** for no. No is the default response. Then, click **OK**. What happens next depends on your response.

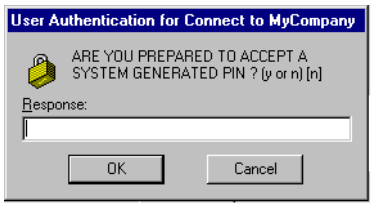
– *If you responded yes* — enter your new pin in the **New Pin** field (Figure 4-11) and enter it again in the **Confirm Pin** field. Click **OK**.

Figure 4-11: Entering a New PIN yourself


User Authentication for Connect to MyCompany
Enter your new Access PIN, containing 4 to 8 digits or 'x' to cancel the new PIN procedure:
New Pin:
****
Confirm Pin:
****
OK
Cancel

– *If you responded no* — the authentication program asks if you will accept a system-generated PIN (Figure 4-12).

Figure 4-12: Accepting a PIN from the system


User Authentication for Connect to MyCompany
ARE YOU PREPARED TO ACCEPT A SYSTEM GENERATED PIN ? (y or n) [n]
Response:
OK
Cancel

2 To receive a PIN, you must respond **y** for yes and then click **OK**. When you do, the authentication program generates a PIN for you and displays it (Figure 4-13). Be sure to remember your PIN.

Figure 4-13: New PIN received

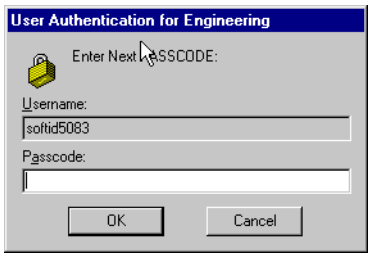
3 To continue, click **OK**.

SecurID Next Cardcode Mode

Sometimes SecurID authentication prompts you to enter the next cardcode from your token card, as in Figure 4-14. SecurID displays this prompt either to resynchronize the token card with the RSA server, or because it noticed several unsuccessful attempts to authenticate with this username.

The **SecurID Next Cardcode Mode** dialog may appear.

Figure 4-14: SecurID Next Cardcode mode dialog



In the **Passcode** field, enter the next code from your token card. This field requires only a cardcode. Do not include your PIN as part of the passcode.

Continue to *Completing the private network connection*.

Using digital certificates

Before you create a connection entry using a digital certificate, you must have already enrolled in a Public Key Infrastructure (PKI), have received approval from the Certificate Authority (CA), and have one or more certificates installed on your system. If this is not the case, then you need to obtain a digital certificate. In many cases, the network administrator of your organization can provide you with a certificate. If not, then you can obtain one by enrolling with a PKI directly using the Certificate Manager application. Currently, we support the following PKIs:

- UniCERT from Baltimore Technologies (www.baltimoretechnologies.com).
- Entrust/PKI™ from Entrust Technologies (www.entrust.com).
- Cybertrust Enterprise CA™ from GTE Cybertrust (www.cybertrust.com).
- Versign (www.verisign.com)
- Microsoft Certificate Services in Microsoft Windows 2000 Server.

The websites listed in parentheses in this list contain information about the digital certificates that each PKI provides. The easiest way to enroll in a PKI or import a certificate is to use the Certificate Manager (see Chapter 6, *Enrolling and managing certificates*).

Note: Every time you connect using a certificate, the VPN Client checks to verify that your certificate has not expired. If your certificate is within one month of expiring, the VPN Client displays a message when you attempt to connect or when you use the Properties option. The message displays the certificate common name, the “not before” date, the “not after” date, and the number of days until the certificate expires or since it has expired.

What happens when you press the **Connect** button can depend on the level of private key protection on your certificate. If your certificate is password protected, you are prompted to enter the password.

Completing the private network connection

After completing the user authentication phase, the VPN Client continues negotiating security parameters and displays a dialog (Figure 4-15). The title bar identifies the remote Cisco VPN device you are connecting to.

Figure 4-15: Completing connection history

If the network administrator of the Cisco VPN device has created a client banner, you see a message designated for all clients connecting to that device; for example, `The Documentation Server will be down for routine maintenance on Sunday`.

After you complete your connection, the VPN Client minimizes to an icon in the system tray on the Windows taskbar.

You are now connected securely to the private network via a tunnel through the Internet, and you can access the private network as if you were an on-site user.

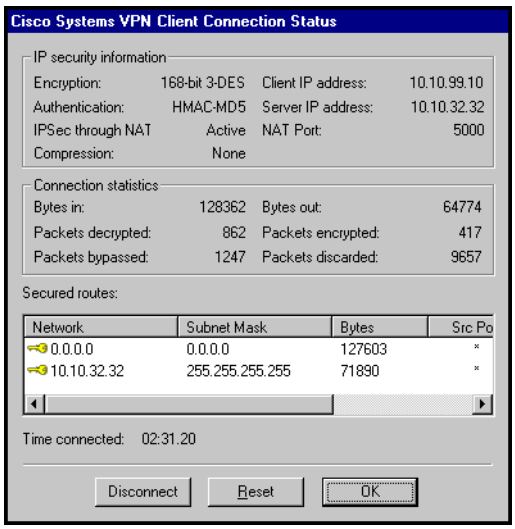
Viewing connection status

The VPN Client icon on the taskbar lets you view the status of your private network connection.

- Double-click the icon, or
- Click the icon with the right mouse button and select **Status** from the pop-up menu.

The **VPN Client Connection Status** dialog appears (Figure 4-16).

Figure 4-16: VPN Client Connection Status dialog



The **Connection Status** dialog provides IP security information, connection statistics, and information about secure routes for your VPN tunnel connection.

IP security information

The **IP security information** section lists the IPSec parameters that govern the use of this VPN tunnel to the private network.

Encryption = The data encryption method for traffic through this tunnel. Encryption makes data unreadable if intercepted.

Authentication = The data, or packet, authentication method used for traffic through this tunnel. Authentication verifies that no one has tampered with data.

Client IP address = The IP address assigned to the VPN Client for the current session.

Server IP address = The IP address of the VPN device to which the VPN Client is connected.

IPSec through NAT = The status of IPSec through NAT mode in the client, either active or inactive.

NAT Port = If **IPSec through NAT** mode is active, the UDP port through which packets are using. This port number comes from the VPN device. If **IPSec through NAT** mode is inactive, then the value of **NAT Port** is zero.

Compression = Whether data compression is in effect as well as the type of compression in use. Currently, the type of compression is LZS.

Connection statistics

The **Connection statistics** section shows statistics for data packets that the VPN Client has processed during the current session or since the statistics were reset. Reset affects only this part of the connection status screen.

Bytes in = The total amount of data received after a secure packet has been successfully decrypted.

Bytes out = The total amount of encrypted data transmitted through the tunnel.

Packets decrypted = The total number of data packets received on the port.

Packets encrypted = The total number of secured data packets transmitted out the port.

Packets bypassed = The total number of data packets that the VPN Client did not process because they did not need to be encrypted. Local ARPs and DHCP fall into this category.

Packets discarded = The total number of data packets that the VPN Client rejected because they did not come from the secure VPN device gateway.

Secured routes

The **Secured routes** section lists the IPSec Security Associations (SAs).

The columns in the display show the following types of information:

Key icon = In the first row shown in Figure 4-16, you see a key at the start of the connection entry. This key shows that the route is secure. The software generates a key as soon as the client needs to send secure data through the tunnel to the networks on the other side. The absence of a key means that the SA is no longer active. The SA may have timed out due to inactivity. Sending data to this network re-establishes the SA, and the key reappears.

Network = The IP address of the remote private network with which this VPN Client has an SA.

Subnet Mask = The subnet mask of the IP address for this SA.

Bytes = The total amount of data this SA has processed. This includes data before encryption as well as encrypted data received.

Src Port, **Dst Port**, and **Protocol** are for future use.

Time connected

The **Connection Status** screen also displays the time in days, hours, minutes and seconds, that has elapsed since you initiated the connection.

Resetting statistics

To reset all **Connection statistics** to zero, click **Reset**. *There is no undo*. **Reset** affects only the connection statistics, not the other sections of this dialog.

Closing the VPN Client

You may want to close the VPN Client when it is running on your PC but not connected to a remote network.

To close the VPN Client when it is not connected to a remote network:

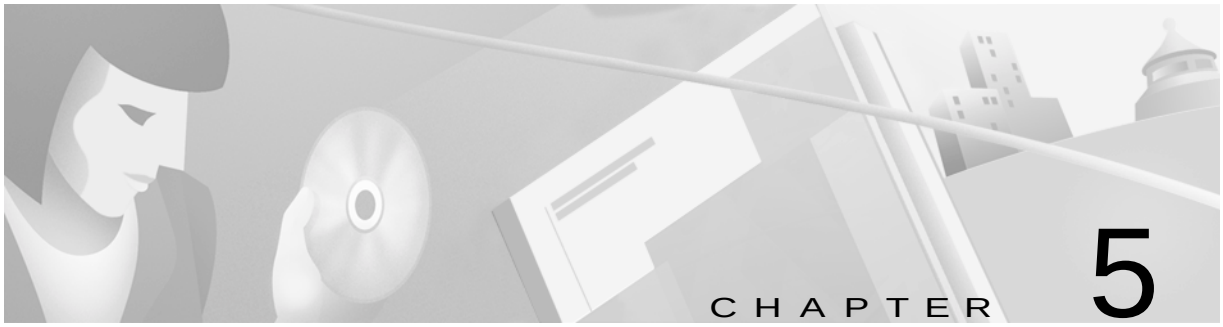
- Click **Close** on the VPN Client's main dialog (see Figure 4-1), or
- Press **Esc** on your keyboard, or
- Press **Alt**-**F4** on your keyboard.

Disconnecting your VPN Client connection

To disconnect your PC from the private network, you can do one of the following:

- Double-click the VPN Client icon on the Windows taskbar. Click **Disconnect** on the **Connection Status** dialog (Figure 4-16).
- Click the VPN Client icon with the secondary mouse button and select **Disconnect** from the pop-up menu.

Your IPSec session ends and the VPN Client closes. You must manually disconnect your dial-up networking connection (DUN).



Managing the VPN Client

This chapter explains how to:

- Manage configured VPN Client connection entries:
  - Clone Entry.
  - Delete.
  - Rename.
  - Create a shortcut.
- On a Windows NT or Windows 2000 system, automatically initiate connections before logging on.
- Launch an application from the logon desktop
- Import a configuration file.
- Automatically configure the VPN Client.
- Use the Log Viewer to examine events in the events log.
- Install a new version of the VPN Client software on your PC.
- Uninstall the VPN Client.

To configure properties of connection entries, see Chapter 3.

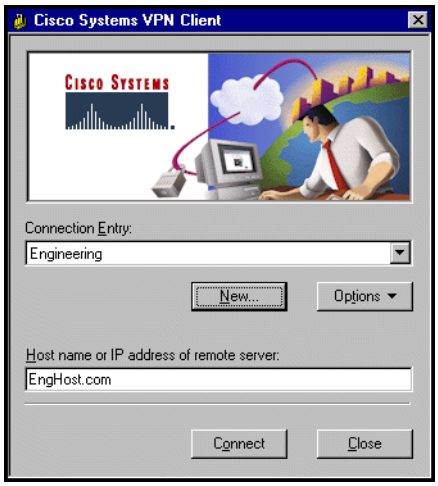
If you are a system administrator, see *VPN Client Administrator Guide* for information on configuring the VPN Concentrator and preparing preconfigured profiles for VPN Clients for users.

Managing connection entries

To manage a connection entry, start the Cisco VPN Client and select **VPN Dialer** from the menu of applications.

The **VPN Client Connect** dialog appears (Figure 5-1).

Figure 5-1: VPN Dialer Connect dialog



Click the **Connection Entry** drop-down menu button and select an entry.

Click **Options** to display the menu.

Figure 5-2: VPN Client Options menu

Cloning a connection entry

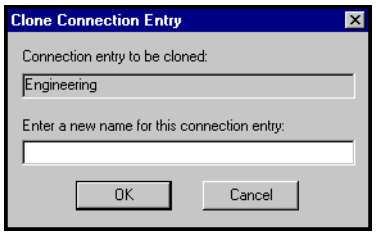
You can clone a connection entry with all its properties and use it as the basis for creating a new one.

1 On the VPN Client's main dialog, click the **Connection Entry** drop-down menu button and select the entry you want to clone.

2 On the VPN Client **Options** menu (Figure 5-2), select **Clone Entry**.

The **Clone Connection Entry** dialog appears (Figure 5-3).

Figure 5-3: Clone Connection Entry dialog



3 Enter a name for the new connection entry in the field and click **OK**.

The dialog closes. The new name appears in the **Connection Entry** list in the VPN Client main dialog.

4 To configure the properties of this new connection entry, click **Options > Properties** on the VPN Client main dialog and see "Setting or changing connection entry properties" in Chapter 3.

Deleting a connection entry

To delete a configured connection entry, follow these steps:

1 On the VPN Client's main dialog, click the **Connection Entry** drop-down menu button and select the entry you want to delete.

2 On the VPN Client **Options** menu (Figure 5-2), select **Delete**.

A confirmation dialog appears (Figure 5-4).

Figure 5-4: Delete dialog

3 Click the appropriate button:

- To permanently delete the connection entry, click **Yes.** *There is no undo.*
- To retain the connection entry, click **No**.

The VPN Client returns to its main dialog.

Renaming a connection entry

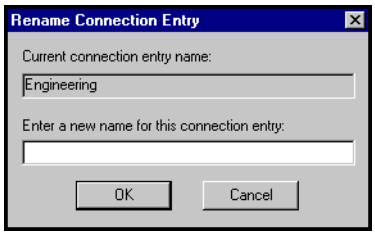
You can rename a connection entry and retain all its properties. Each connection entry name must be unique. Since these names are *not* case-sensitive, be sure the new name differs in content, not just case.

1 On the VPN Client's main dialog, click the **Connection Entry** drop-down menu button and select the entry you want to rename.

2 On the VPN Client **Options** menu (Figure 5-2), select **Rename**.

The **Rename Connection Entry** dialog appears (Figure 5-5).

Figure 5-5: Rename Connection Entry dialog



3 Enter a new name for this connection entry in the field and click **OK**.

The dialog closes. The new name appears in the **Connection Entry** list in the VPN Client main dialog.

Creating a shortcut for a connection entry

You can create a shortcut on your desktop to quickly and directly launch a VPN Client connection entry that you use frequently.

1 On the VPN Client's main dialog, click the **Connection Entry** drop-down menu button and select an entry.

2 On the VPN Client **Options** menu (Figure 5-2), select **Create Shortcut**.

The shortcut appears on your desktop, as in this example (Figure 5-6).

Figure 5-6: Connection entry shortcut

The VPN Client main dialog remains open.

Importing a VPN Client Configuration File

You can automatically configure your VPN Client with new settings by importing a new configuration file (a file with a `.pcf` extension, called a *profile*) that your system administrator supplies.

To automatically configure a VPN Client:

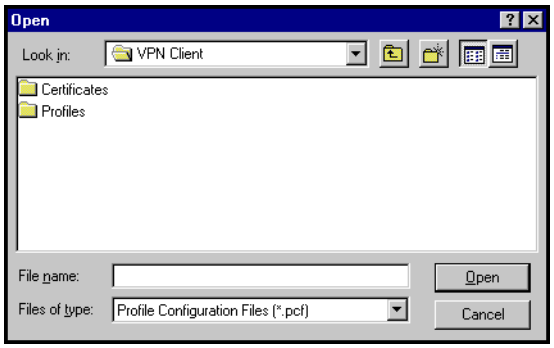
1 Obtain a new VPN Client profile (`.pcf`) file from your system administrator.

2 Load the file on your hard disk.

3 On the **VPN Client** main dialog, click **Options** and select **Import** from the menu.

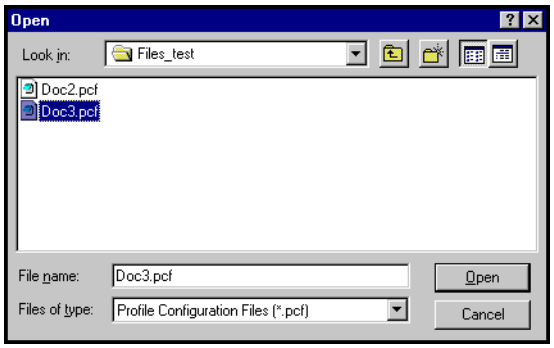
The VPN Client opens a window for you to select the profile file (Figure 5-7).

Figure 5-7: Selecting a file to import



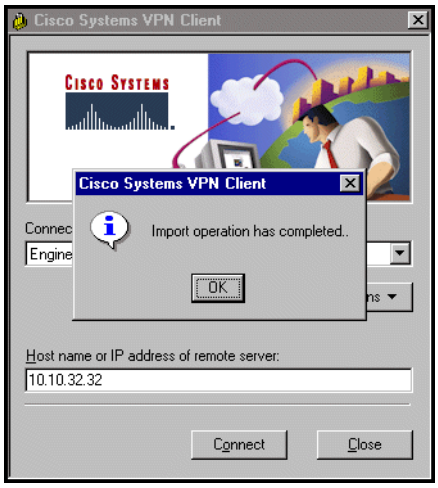
4 Browse until you locate the profile file and when you have located it, select it and click **Open** (Figure 5-8).

Figure 5-8: Importing the profile file



The VPN Client displays a message informing you that your file import was successful (Figure 5-9). If the profile already exists, you receive a message asking if you want to overwrite it.

Figure 5-9: Import successful



5 To continue, click **OK**.

Alternatively, you can copy the .pcf file into the Profiles directory and restart the VPN Dialer application.

Your VPN Client is now configured with the connection entries and parameters specified by this new profile file. You can examine or modify the connection entries by clicking the **Connection Entry** drop-down menu button on the main dialog, selecting an entry, and clicking **Options > Properties**.

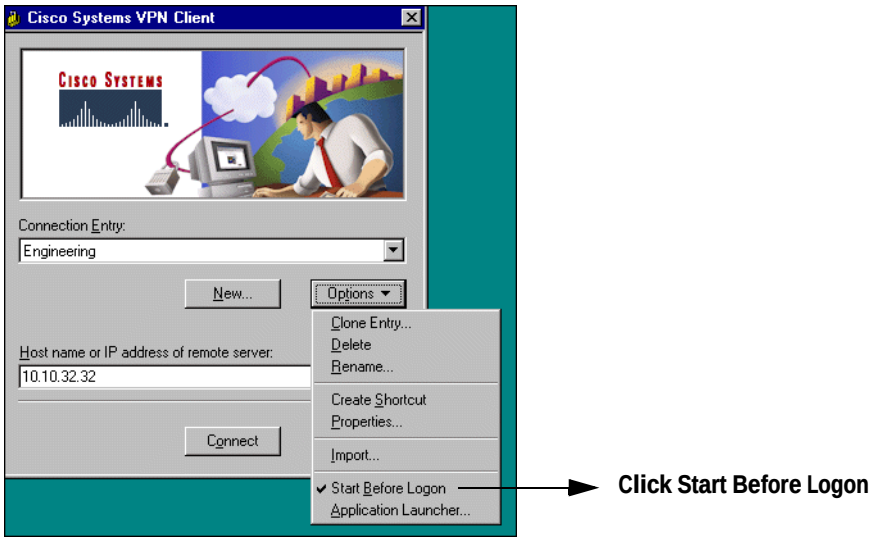
Starting connections before logging on (Windows NT and Windows 2000 only)

You can connect to the private network before you log on to your system. Your administrator may have set this up for you. Once you establish a VPN connection, your credentials are sent to a domain controller for logging in to your system. If you need to launch an application before you logon, see *Launching an application* for information.

When you have established a successful VPN connection, the VPN Dialer window closes and your logon window displays. If the connection is not successful, the VPN Dialer window continues to display. Your administrator may have set up a banner that lets you know when you have a successful connection.

To activate this feature, open the VPN Client **Options** pull-down menu (Figure 5-2) and select **Start Before Logon** (make sure it is checked) (Figure 5-10).

Figure 5-10: Setting up Start Before Logon feature



What happens when you use Start Before Logon

When **Start Before Logon** is active, the following events occur when your system starts:

- First, your system logon dialog displays. There may be other messages that display as well, depending on your setup. You should wait until you see the VPN Dialer start.
- Next, the VPN Dialer starts and displays the connection dialog over the system logon dialog.
- You establish your connection to the private network of the VPN Device.
- Then you log on to your system.

Turning off Start Before Logon

To turn this feature off, open the **Options** pull-down menu on the VPN Dialer connection dialog and uncheck **Start Before Logon**. The next time you start your system, the VPN Dialer connection dialog does not automatically display on your logon desktop.

Note: You can use certificates for authentication with **Start Before Logon** only when your personal certificate along with the CA or intermediary certificate(s) are in your Cisco certificate store (not your Microsoft store). For information on enrolling certificates and importing certificates into your Cisco store, see Chapter 6, *Enrolling and managing certificates*.

Launching an application

You can configure the dialer to automatically launch an application before establishing a connection. Some examples of why you would want to use this feature are:

- You are configured for Start Before Logon and you need to start an authentication application at the logon desktop.
- You want to launch a monitoring application such as the Log Viewer before each connection. (Figure 5-11 through Figure 5-13).

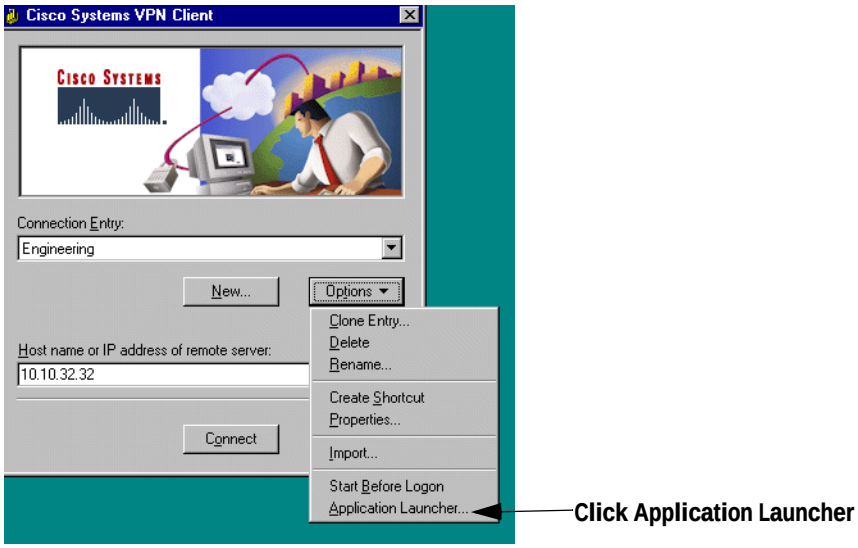
To configure the VPN Dialer to launch an application from the logon desktop, use the **Application Launcher**.

The **Application Launcher** starts the specified application once per session. To launch an application again, you must exit from the VPN Dialer, restart the VPN Dialer, and launch the application.

To activate **Application Launcher**:

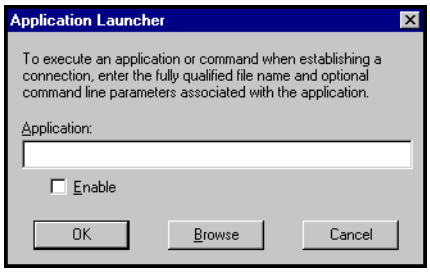
1 Open the VPN Dialer **Options** pull-down menu (Figure 5-2) and click **Application Launcher** (Figure 5-11).

Figure 5-11: Application Launcher option



The VPN Dialer displays a dialog prompting for the name of the application (Figure 5-12).

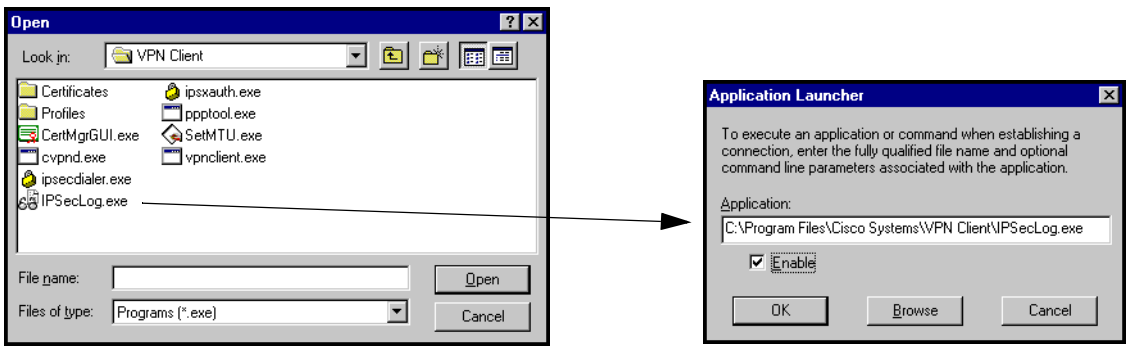
Figure 5-12: Application Launcher dialog


Application Launcher
To execute an application or command when establishing a connection, enter the fully qualified file name and optional command line parameters associated with the application.
Application:
Enable
OK
Browse
Cancel

2 Click **Browse** to locate and then select the complete pathname to the application as well as the name of the application (Figure 5-13).

The application name appears in the **Application Launcher** dialog. In this example, the VPN Dialer is configured to launch the Log Viewer before a connection.

Figure 5-13: Selecting an application



3 Click **Enable** and then click **OK**.

Turning off Application Launcher

To disable **Application Launcher**:

1 Open the **Options** pull-down menu and select **Application Launcher**.

2 When the **Application Launcher** dialog displays, remove the check from in front of **Enable**.

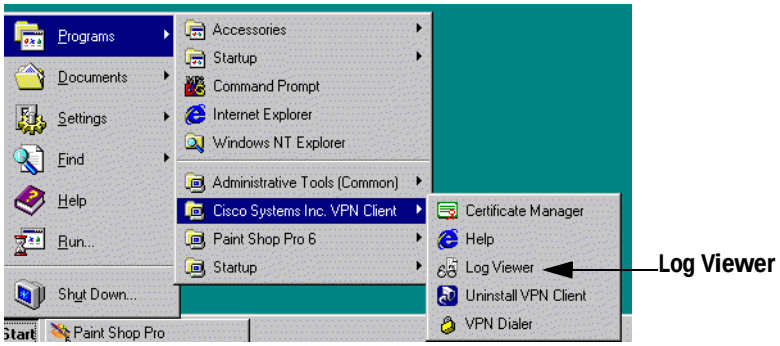
Viewing and managing the VPN Client event log

Examining the event log can often help a network administrator diagnose problems with an IPSec connection between a VPN Client and a peer device. The log view application collects event messages from all processes that contribute to the client-peer connection. This section shows how to use the Log Viewer to retrieve and manage this information.

Starting the Log Viewer

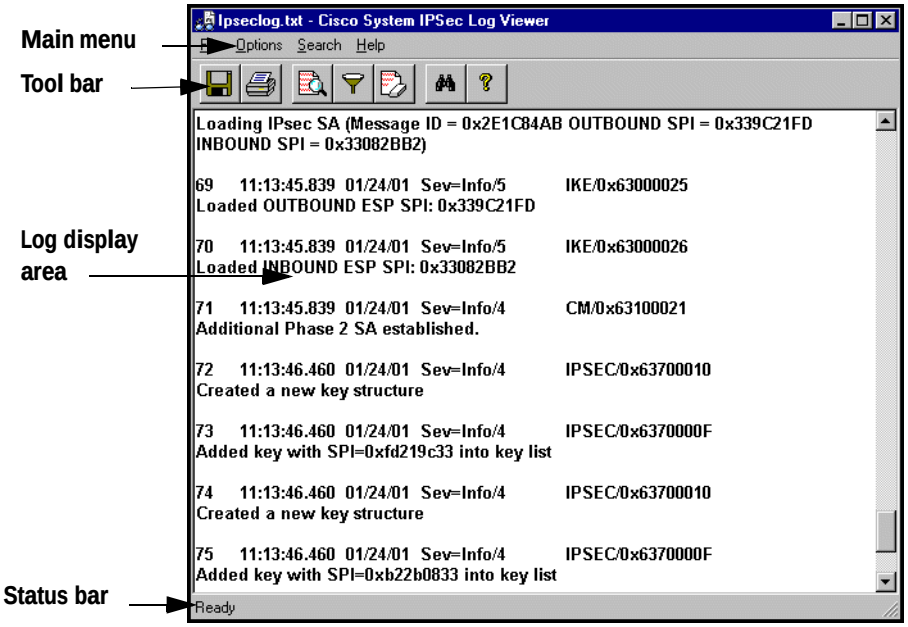
To start the Log Viewer, use the following path from the **Start** menu (Figure 5-14): **Start > Programs > Cisco Systems VPN Client > Log Viewer**.

Figure 5-14: Starting the Log Viewer



The Log Viewer starts, displaying its main window (Figure 5-15). By default, the filter is set to low, so you may not see any events displayed in this window (see *Filtering events*).

Figure 5-15: Log viewer main window


Main menu
Tool bar
Log display area
Status bar
Ipseclog.txt - Cisco System IPSec Log Viewer
Options Search Help
Loading IPsec SA (Message ID = 0x2E1C84AB OUTBOUND SPI = 0x339C21FD INBOUND SPI = 0x33082BB2)
69 11:13:45.839 01/24/01 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x339C21FD
70 11:13:45.839 01/24/01 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x33082BB2
71 11:13:45.839 01/24/01 Sev=Info/4 CM/0x63100021
Additional Phase 2 SA established.
72 11:13:46.460 01/24/01 Sev=Info/4 IPSEC/0x63700010
Created a new key structure
73 11:13:46.460 01/24/01 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0xfd219c33 into key list
74 11:13:46.460 01/24/01 Sev=Info/4 IPSEC/0x63700010
Created a new key structure
75 11:13:46.460 01/24/01 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0xb22b0833 into key list
Ready

Displaying the version of the software

To display a brief help message that gives you the version number of the software, select **Help** from the main menu or click the Help icon.

Collecting events

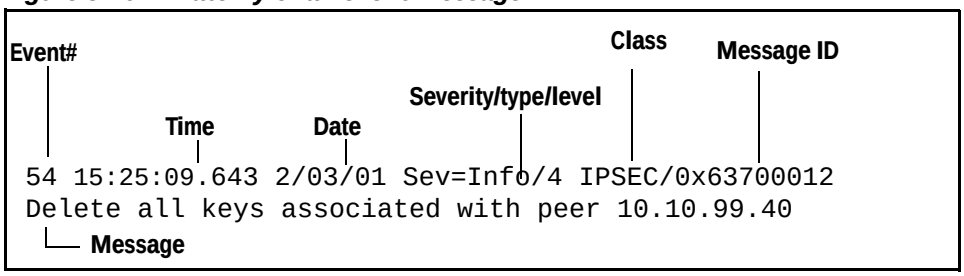
To start collecting event messages into the log file, select **Options > Capture**. When a check mark appears in front of the **Capture** option, Log Viewer is collecting events. This option is off by default. Alternatively, you can click the Capture icon.

Each message in the log file comprises at least two lines containing the following fields:

```
Event# Time Date Severity/type/level EventClass/MessageID
Message text
```

Figure 5-16 shows a sample event message in the log file.

Figure 5-16: Anatomy of an event message



Event#

The first field shows the event number. Events are numbered incrementally and never reset.

Time

The time of the event: *hour:minutes:seconds*. The hour is based on a 24-hour clock. For example `15:25:09` identifies an event that occurred at 3:25:09 PM.

Date

The date of the event: *MM/DD/YYYY.* For example, `2/03/2001` identifies an event that occurred on February 3, 2001.

Severity/type/level

The severity type and level of the event; for example, `Sev=Info/4`, which identifies an informational event, severity level 4. Table 5-1 identifies event types and severity levels.

Table 5-1: Event types and severity levels

Type	Levels	Meaning
Fault	1	A system failure or non-recoverable error.
Warning	2 - 3	Imminent system failure or a serious problem that may require user intervention.
Informational	4 - 6	Level 4 provides the most general type (high level) information. Levels 5 and 6 provide more detailed information about the connection.

Event Class/Message ID

The module or source of the event and the message identifier associated with the module. For example, `IPSEC/0x63700012` (Figure 5-16).

Message text

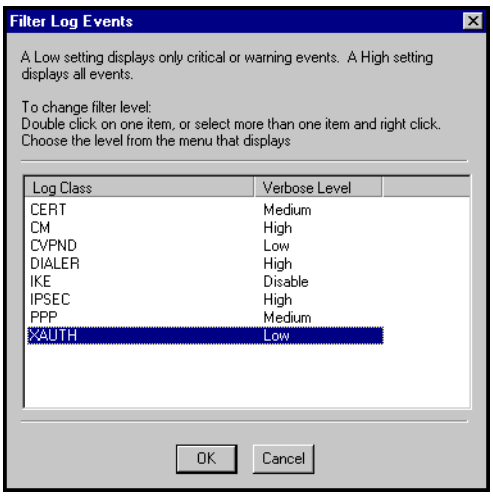
A brief message describing the event. Usually this message is no more than 80 characters. For example, `Delete all keys associated with peer 10.10.99.40`. In a message containing arrows, the arrows indicate the direction of the transmission: >>> for sending and <<< for receiving.

Filtering events

To control the amount of information to view with the Log Viewer, select **Options > Filter**. Alternatively, you can click the Filter icon.

The Log Viewer displays the **Log Viewer Filter** message to let you choose the amount of information you want to capture (Figure 5-17).

Figure 5-17: Log Viewer Filter message



To change the filter level, do the following:

- Double-click on one item, or select more than one item and right click.
- Choose from the following options that the Log Viewer displays:

Disable - inhibits event reporting for the selected class.

Low - provides the least amount of information. This choice includes severity levels 1 through 3 (all faults and warnings). Low is the default for all classes.

Medium - includes severity levels 1 through 4; all in Low plus the first level informational events, which provide general information about the connection. Note that a first level informational event is level 4 and appears in the event display as **Info/4.**

High - includes severity levels 1 through 6, thus adding two levels of informational events (**Info/5** and **Info/6**). This setting can lower the performance of all applications on your system, so use it only when your network administrator or a support engineer suggests that you do so.

Table 5-2 defines the classes (modules) that generate events.

Table 5-2: Classes that generate events in the VPN Client

Class Name	Definition
CERT	Certificate management process, which handles getting, validating, and renewing certificates from certificate authorities. CERT also displays errors that occur as you use the application.
CM	Connection manager, which drives VPN connections. (Dials a PPP device, configures IKE for establishing secure connections, and manages connection states.
CVPND	Cisco VPN Daemon (main daemon), which initializes client service and controls messaging process and flow.
DIALER	Windows-only component, which handles configuring a profile, initiating a connection, and monitoring it.
IKE	Internet Key Exchange module, which manages secure associations.
IPSEC	IPSec module, which obtains network traffic and applies IPSec rules to it.

Table 5-2: Classes that generate events in the VPN Client

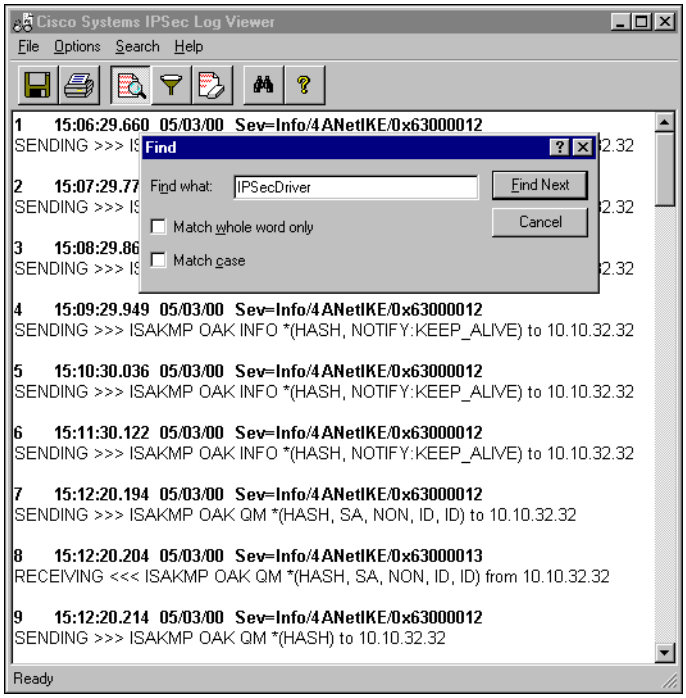
Class Name	Definition
PPP	Point to Point Protocol.
XAUTH	Extended authorization application, which validates a remote user's credentials.

Searching the log file

To locate specific events or event types in the window, select **Search** from the main menu. Alternatively, you can click on the Search icon.

The Log Viewer displays the **Find** message (Figure 5-18). Enter a string to find and click **Find Next**. You can match on whole words and on case.

Figure 5-18: Searching the log display



Printing the log file

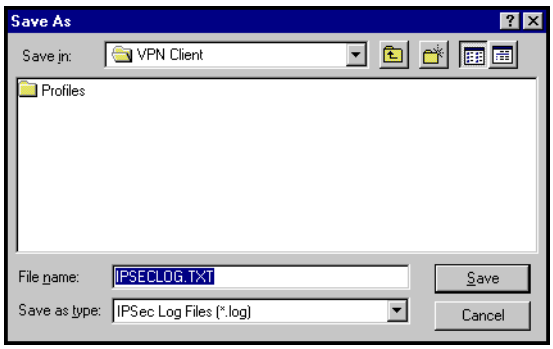
To print the events displayed in the current window, select **File > Print** from the main menu. Alternatively, you can click the Printer icon.

Saving the log file

To save the currently displayed events in the `ipseclog` file on your hard drive, select **File > Save as** from the main menu. Alternatively, click the Disk icon.

The `ipseclog` file is a text (.txt) file in DOS format. The Log Viewer saves the information to the Client install directory, which by default is the pathname `Program Files\Cisco Systems VPN Client \VPN Client\IPSECLOG.TXT`. You can specify any directory and name (Figure 5-19).

Figure 5-19: Saving a log file



Clearing the events display

To eliminate all the events currently displayed in the Log Viewer main window, select **Options > ClearLog Display** from the main menu. Alternatively, you can click the Erase All icon.

If you want to store the event messages, be sure you save them before you clear the display. Clearing the display does not reset event numbering.

Installing a new version of the VPN Client

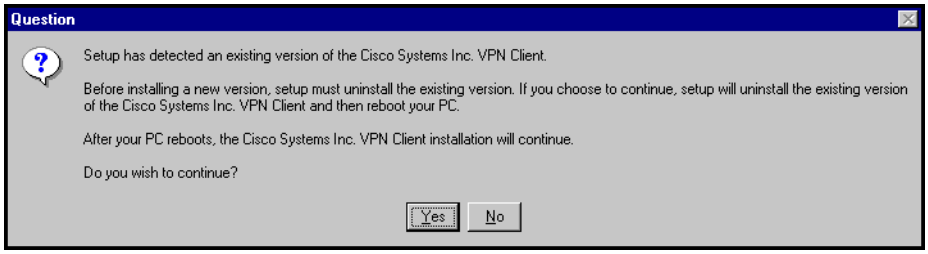
Installing a new version this way retains existing connection entries and their parameters.

To install a new version of the VPN Client over an existing version on your system, use the following procedure, which first uninstalls the existing version, and then reboots your PC and installs the new version.

1 To begin the procedure, follow the instructions under *Installing the VPN Client* on page 2-4.

When it starts, the installation wizard detects the existing version and asks you to confirm that you want to remove that version and reboot your PC (Figure 5-20).

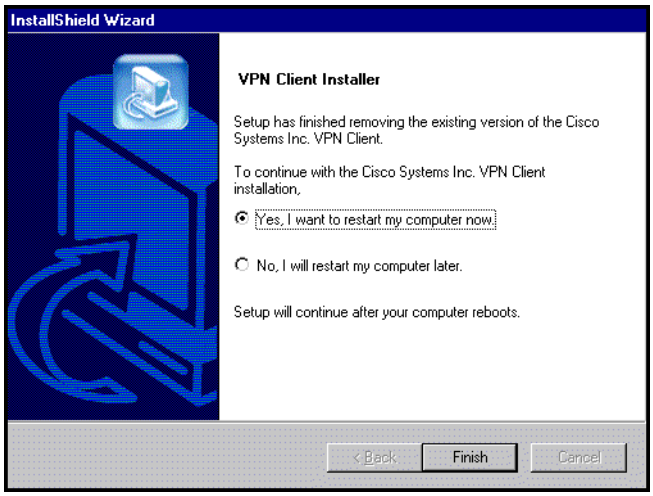
Figure 5-20: Uninstalling an existing version


Question
Setup has detected an existing version of the Cisco Systems Inc. VPN Client.
Before installing a new version, setup must uninstall the existing version. If you choose to continue, setup will uninstall the existing version of the Cisco Systems Inc. VPN Client and then reboot your PC.
After your PC reboots, the Cisco Systems Inc. VPN Client installation will continue.
Do you wish to continue?
Yes
No

2 To continue, click **Yes**.

The installation program removes the old version and asks you to confirm the system restart(Figure 5-21).

Figure 5-21: Confirming the system restart


InstallShield Wizard
VPN Client Installer
Setup has finished removing the existing version of the Cisco Systems Inc. VPN Client.
To continue with the Cisco Systems Inc. VPN Client installation,
Yes, I want to restart my computer now.
No, I will restart my computer later.
Setup will continue after your computer reboots.
< Back
Finish
Cancel

Be sure to remove any diskette from its drive before you restart your system.

If you are installing from diskettes, reinsert Disk 1 after your system restarts and displays the Windows logo screen, but *before* the desktop appears.

3 To restart your system, click the **Yes** radio button (the default) and click **Finish**.

The installation wizard restarts your system. Once your system has restarted, installation continues automatically.

4 Follow the instructions as if you were installing for the first time. See *Installing the VPN Client* on page 2-4.

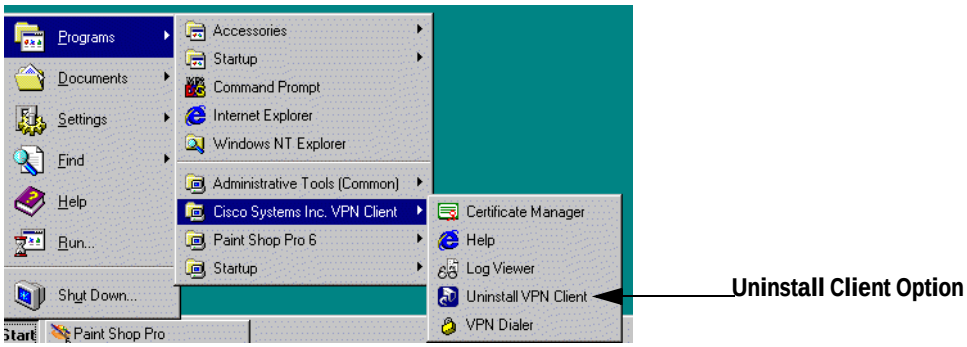
Uninstalling the VPN Client

Uninstalling the VPN Client means completely removing all VPN Client software from your computer. For example, if you are changing or upgrading your PC, you might want to uninstall the VPN Client.

Before you run the uninstall program, make sure you have closed all of your remote access (Dial-Up Networking) connections and all VPN Client applications. Then use the following procedure (Figure 5-22).

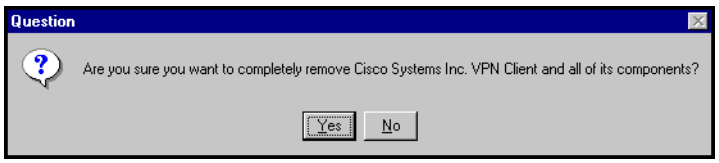
1 Select **Start > Programs > Cisco Systems VPN Client > Uninstall VPN Client**.

Figure 5-22: Running the Uninstall program



The Uninstall Wizard runs and asks if you want to really want to remove the VPN Client applications (Figure 5-23).

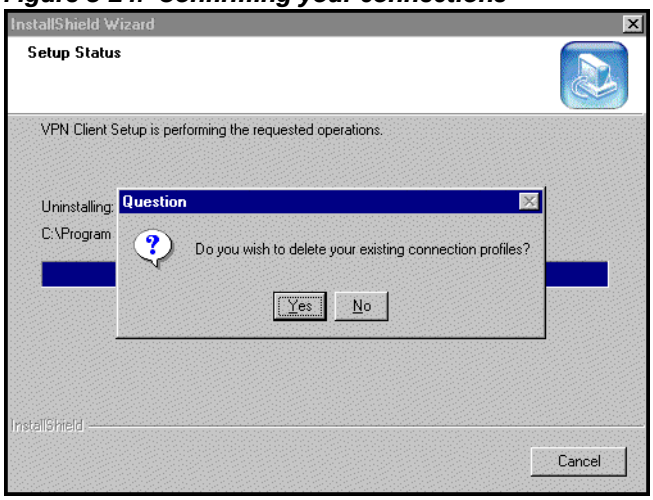
Figure 5-23: Confirming uninstall



2 To completely remove the VPN Client software from your system, click **Yes**. Otherwise, click **No**.

Next, the Uninstall Wizard asks if you want to delete your connection profiles (Figure 5-24).

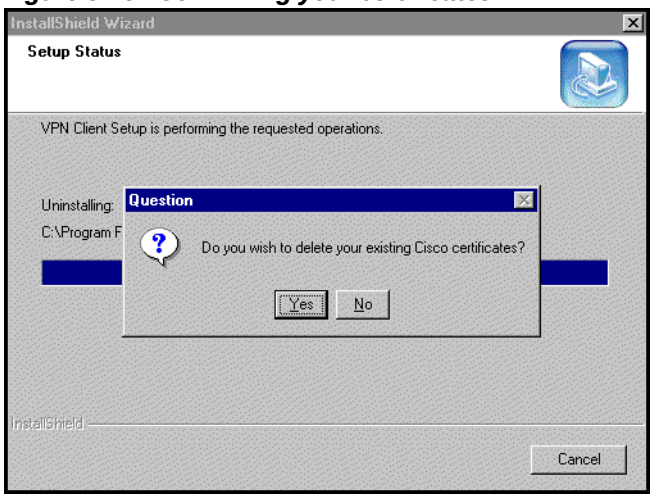
Figure 5-24: Confirming your connections



3 To preserve your connection profiles (which contain configured connection entries), click **No**.

Then the Uninstall Wizard asks if you want to delete your certificates (Figure 5-25).

Figure 5-25: Confirming your certificates



4 To keep your certificates, click **No**.

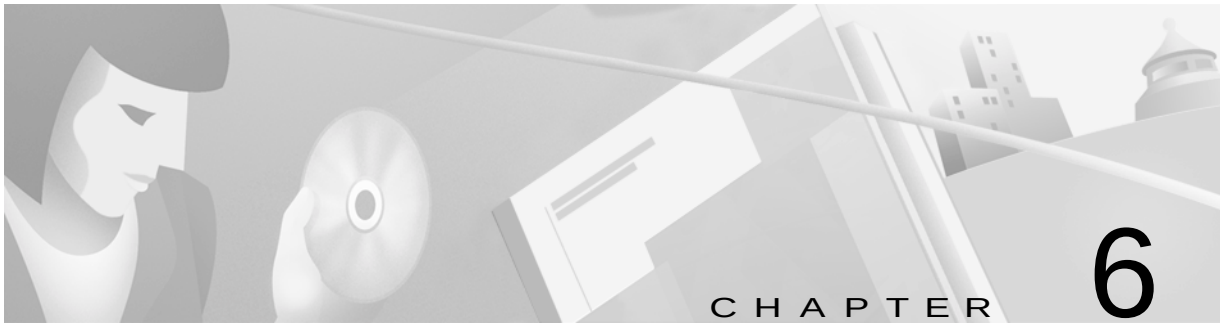
Finally, the Uninstall Wizard prompts you to restart your system. To complete the uninstallation, you must restart your system.

5 To restart your system, click **Yes** (the default) and then click **Finish**.

The installation program restarts your system.

Be sure to remove any diskette from its drive before you restart your system.

Note: When you uninstall the VPN Client software after you have run the Log Viewer and you have clicked yes to remove your certificate and profile directories, the `vpnclient.ini` and `ipseclog.txt` files remain on your system. Since these files were generated after you installed the software, they are not removed when you uninstall the software.



Enrolling and managing certificates

This chapter explains how to enroll and manage personal certificates using the Certificate Manager application specifically, how to:

- Obtain personal certificates through enrollment with a Certificate Authority (CA), which is an organization that issues digital certificates that verify that you are who you say you are.

  You can enroll for a certificate in two ways:

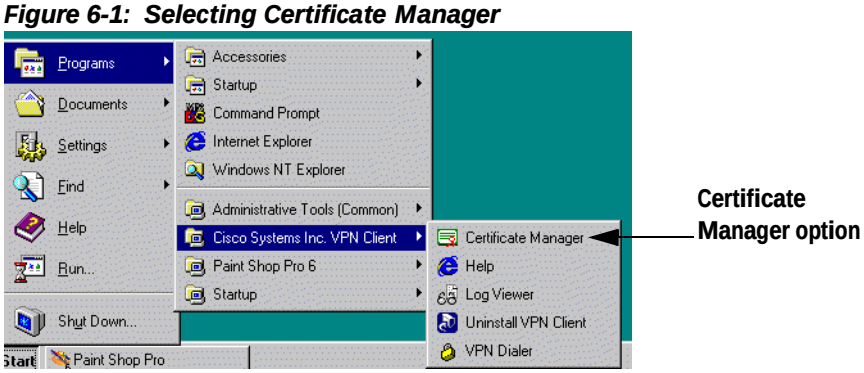
  – through the network (*online enrollment)*

  – via a file
- Import certificates
- Manage certificates
  – Viewing
  – Verifying
  – Deleting
  – Exporting
- Manage enrollment requests

To get started with certificates, go to the **Cisco Systems VPN Client** menu (the same menu that you use to start the client, shown in Figure 6-1).

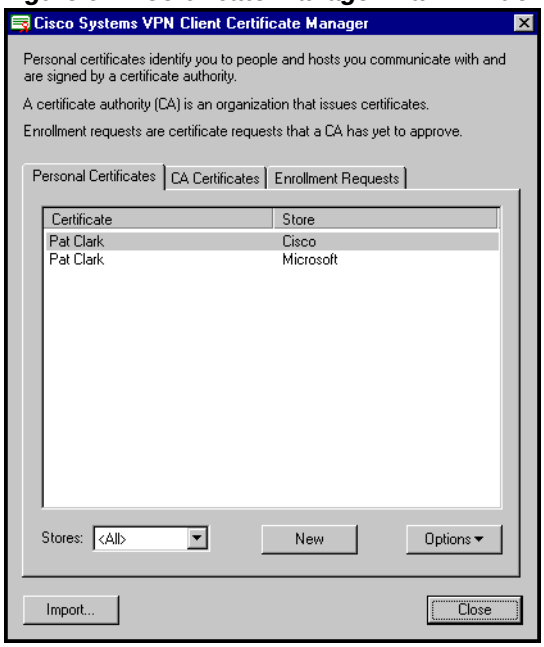
Select **Start> Programs> Cisco Systems VPN Client> Certificate Manager**.

Figure 6-1: Selecting Certificate Manager



The **Certificate Manager** window opens (Figure 6-2).

Figure 6-2: Certificate Manager main window



Certificate stores -- what are they?

The Certificate Manager uses the notion of *store* to convey a location in your local file system for storing personal certificates. The major store for the VPN Client is the Cisco store. The Cisco store contains certificates you have enrolled for through the Simple Certificate Enrollment Protocol (SCEP). This application supports several standard enrollment protocols. Your system also includes a Microsoft certificate store that may contain certificates that your organization provides or that you have installed previously. You can manage them just like the certificates in your Cisco store, or you can import them to your Cisco store. New certificates obtained through enrollment or importing go into the Cisco store.

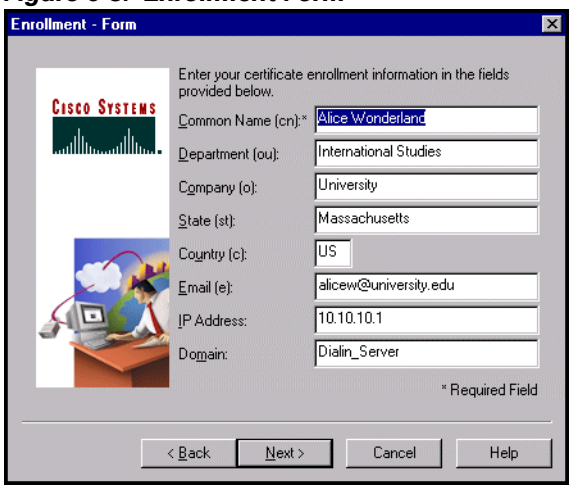
Enrolling for a certificate

Your system administrator may have already set up your VPN Client with digital certificates. If not, or if you want to add certificates, you can obtain a certificate by enrolling with a CA over the network or by creating a file request. In both cases, you complete the same form (shown in Figure 6-3).

Enrollment form

This section describes the information you'll need for filling out the certificate enrollment form. Make sure you have all of the following information before you start.

Figure 6-3: Enrollment Form



- **Common Name**: Your *common name* (CN), which is the unique name to use for this certificate. This field is required. The common name can be the name of a person, system, or other entity; it's the most specific level in the identification hierarchy. The common name becomes the name of the certificate; for example, `Alice Wonderland`.
- **Department**: The name of the department to which you belong; for example, `International Studies`. This field correlates to the Organizational Unit (OU). The OU is the same as the Group Name configured in a VPN 3000 Series Concentrator, for example.
- **Company**: The name of the company or organization (O) to which you belong; for example, `University`.
- **State**: The name of your state (ST); for example, `Massachusetts`.
- **Country**: The 2-letter country code for your country (C); for example, `US`. This two-letter country code must conform to ISO 3166 country abbreviations.
- **Email**: Your email address (e); for example, `alicew@university.edu`.
- **IP Address**: The IP address of your system, for example, `10.10.10.1`.
- **Domain**: The Fully Qualified Domain Name of the host for your system; for example, `Dialin_Server`.

Together all these fields except IP address and domain comprise your *distinguished name* (DN).

When you enroll a personal certificate, you either go through a CA from which your system already has a root certificate or you obtain a root certificate from the CA as part of the enrollment process. The **CA Certificates** tab displays the current list of CA certificates (Figure 6-2).

Starting enrollment

To begin, click **New** on the Certificate Manager's main screen under the **Personal Certificates** tab (Figure 6-2). The Certificate Manager prompts you to enter a password for the certificate you are enrolling (Figure 6-4). The password is optional, but we recommend that you use one to protect your private key more effectively. The password can be up to 32 characters in length. Passwords are case sensitive. For example, *sKate8* and *Skate8* are different passwords. This password becomes the *personal certificate password*.

Figure 6-4: Protecting a certificate with a password

Certificate Password Protection
Cisco Systems
Password protecting your certificate provides an additional level of security. This password is optional.
By choosing to protect your certificate with a password, any operation that requires access to the certificate's private key will require the specified password to continue.
Note - File based enrollments require the password used here to be re-entered when the approved certificate is imported.
Password:
Confirmation Password:
< Back
Next >
Cancel
Help

After entering a password, click **Next** to continue. The Certificate Manager lets you select between enrolling via the network or by creating a file (Figure 6-5). Enrolling via the network is also called *online enrollment*.

Figure 6-5: Selecting enrollment method

Enrollment - Network or File
Cisco Systems
The enrollment wizard allows you to request a personal identity certificate from a Certificate Authority (CA).
Network based enrollment allows you to connect directly to a CA over a network connection.
File based enrollment will produce a certificate request file which you need to submit to your administrator.
Please select the method you wish to proceed with:
Enrollment type:
Network
File
< Back
Next >
Cancel
Help

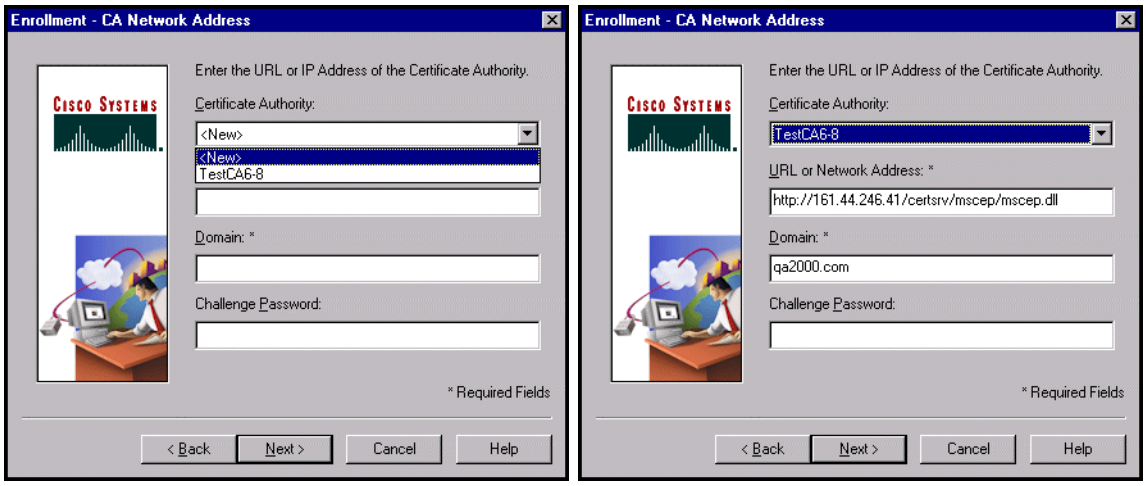
Enrolling via the network

Enrolling through the network retrieves a certificate from a CA and places it in the Cisco store.

Use the following procedure:

1 Click the **Network** radio button (Figure 6-5) and click **Next**. The Certificate Manager asks you to enter the network address of the issuing certificate authority (Figure 6-6).

Figure 6-6: Entering network address



2 Do one of the following:

- Select an existing **Certificate Authority** from the drop down menu.
  - The **URL or Network Address** and **Domain** fields are automatically filled.
  - Renter the **Challenge password** or enter a new password, which you can obtain from the CA or your network administrator.
- Select **<New>** from the drop down menu.
  - Enter the **URL or Network Address** of the CA and the CA's **Domain**, both of which are required.
  - Some CAs require that you enter a password to access their site. If this is the case, enter the password in the **Challenge Password** field. You can get the password from the CA or from your network administrator.

3 When you have completed the network address information, click **Next>**.

The Certificate Manager displays the enrollment form for you to complete (Figure 6-3).

4 Enter the information you collected before you started the enrollment process. The only field that the Certificate Manager requires is **Common Name.** However the CA may require some or all of the other fields. Then click **Next>.**

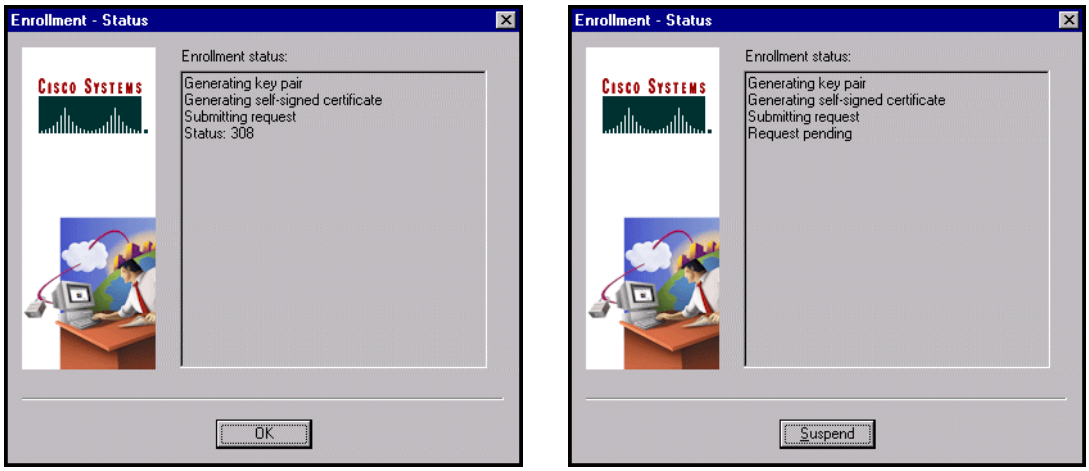
- After you enter the form, the Certificate Manager displays a summary that looks something like the one in Figure 6-7.

Figure 6-7: Enrollment summary

5 To complete the enrollment, click **Finish**.

– The Certificate Manager displays a status window (Figure 6-8) that lets you monitor the progress of the certificate retrieval. If the enrollment failed, the status window indicates the cause so you can fix the problem and try again.

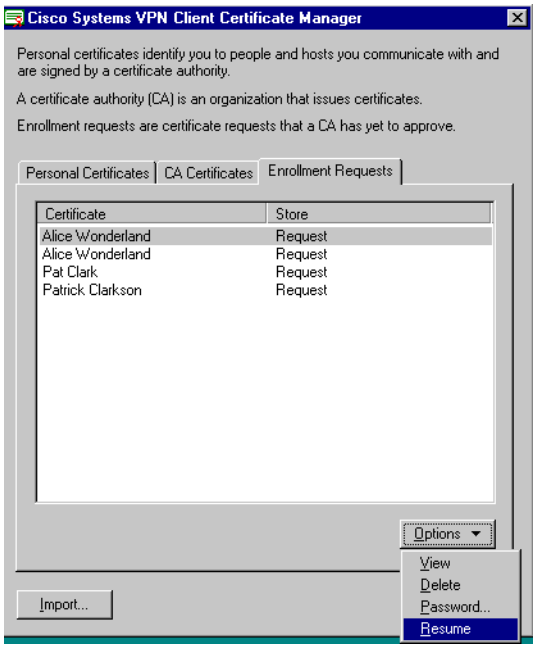
Figure 6-8: Certificate status messages



6 What happens next depends on your CA (Figure 6-8):

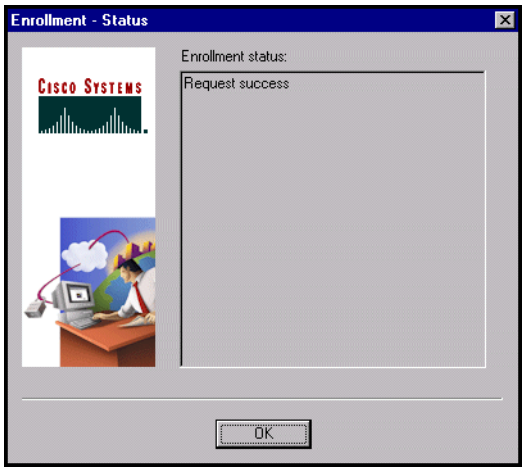
- Some CAs may provide immediate response. If so, the **Enrollment - Status** window reflects this fact and displays an **OK** button.
  – Click **OK** and you see a message that your enrollment succeeded. You can view and manage the certificate under the **Personal Certificates** tab.
- If the enrollment status is `Request pending`, your CA does not immediately approve your request and the **Enrollment - Status** window shows the **Suspend** button.
  – Click the **Suspend** button.
  – Your request appears under the **Enrollment Requests** tab, while you are waiting for the CA to issue the certificate.
  – When the CA issues your certificate, select the certificate and then select **Resume** from the **Options** pull-down menu to complete the enrollment (Figure 6-9).

Figure 6-9: Resuming enrollment request



– After you have obtained the certificate, the status screen updates to show the result (Figure 6-10).

Figure 6-10: Receiving status update



7 Click the **OK** button.

Enrolling via a file request

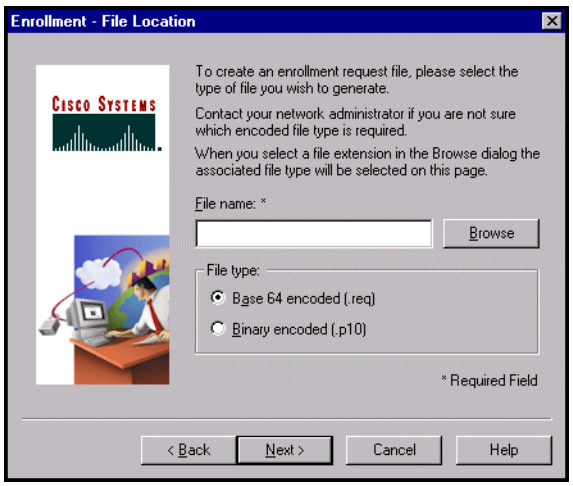
Alternatively, you can enroll by creating a file, using the same form as network enrollment (Figure 6-3). Once you have created a request file, you can either email it to the CA and receive a certificate back or you can access the CA's website and cut and paste the enrollment request in the area that the CA provides.

Use the following procedure:

1 At the **Selecting method of enrollment** dialog (Figure 6-5), click the **File** radio button and click **Next**.

The Certificate Manager prompts you to select a file type for your file request and to specify a file name (Figure 6-11).

Figure 6-11: Selecting file type and location

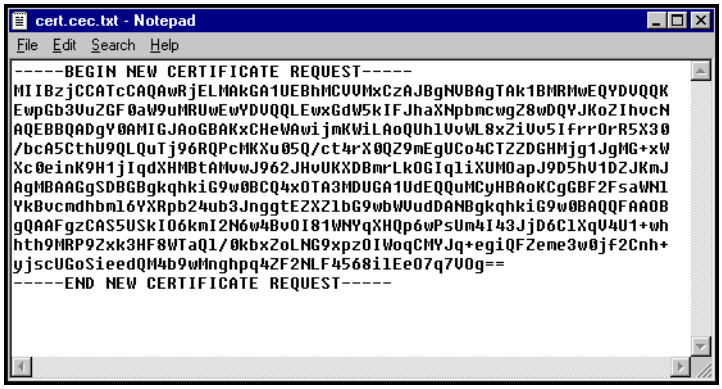

Enrollment - File Location
Cisco Systems
To create an enrollment request file, please select the type of file you wish to generate.
Contact your network administrator if you are not sure which encoded file type is required.
When you select a file extension in the Browse dialog the associated file type will be selected on this page.
File name: *
Browse
File type:
Base 64 encoded (.req)
Binary encoded (.p10)
* Required Field
< Back
Next >
Cancel
Help

2 Click one of the following file types:

– **Binary encoded**, a base-2 PKCS10 file (Public Key Cryptography Standard) (for example, an X.509 DER file). You can't display a binary-encoded file.

– **Base 64 encoded**, an ASCII-encoded PKCS10 file that you can display because it is in text format (such as the request in Figure 6-12). Select this type when you want to cut and paste the text into the CA's website.

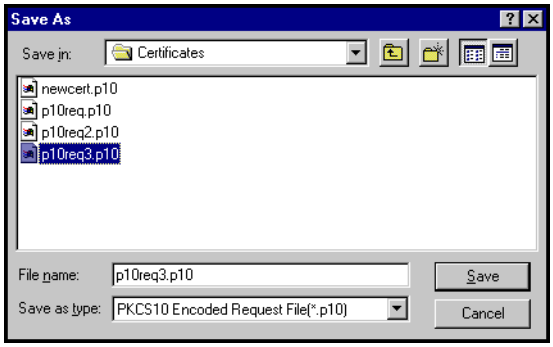
Figure 6-12: A PKCS10 certificate request



3 Enter the full pathname for the file request.

When you browse for an appropriate directory for placing the file request, the Certificate Manager shows only the files of the selected file type (Figure 6-13). You can save your file enrollment requests in the `Certificates` directory, which is a subdirectory of where the VPN Client is installed.

Figure 6-13: Specifying a filename

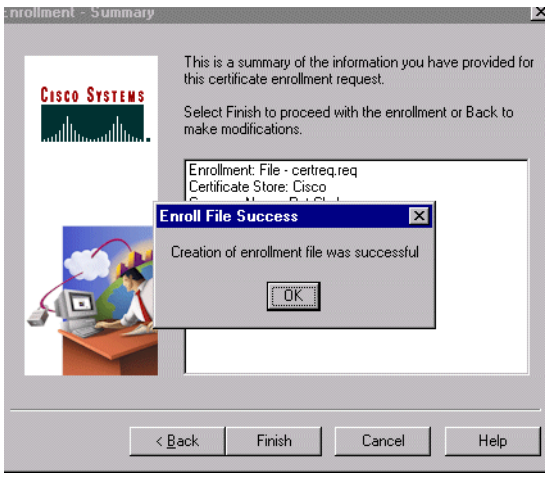


In this example, the complete pathname is `C:\Program Files\Cisco Systems\VPN Client\Certificates\p10req3.p10.`

4 Complete the form (see *Enrollment form*) and click **Next>**.

The Certificate Manager displays the summary screen and a message to let you know that your request succeeded (Figure 6-14).

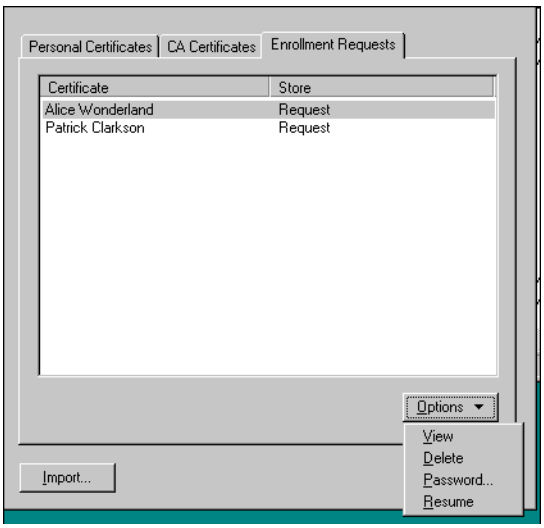
Figure 6-14: Enroll File Success message


This is a summary of the information you have provided for this certificate enrollment request.
Select Finish to proceed with the enrollment or Back to make modifications.
Enrollment: File - certreq.req
Certificate Store: Cisco
Enroll File Success
Creation of enrollment file was successful
OK
< Back
Finish
Cancel
Help

5 Click **OK** on the message screen then click **Finish** on the summary screen.

You can view the file request under the **Enrollment Requests** tab (Figure 6-15).

Figure 6-15: File enrollment requests



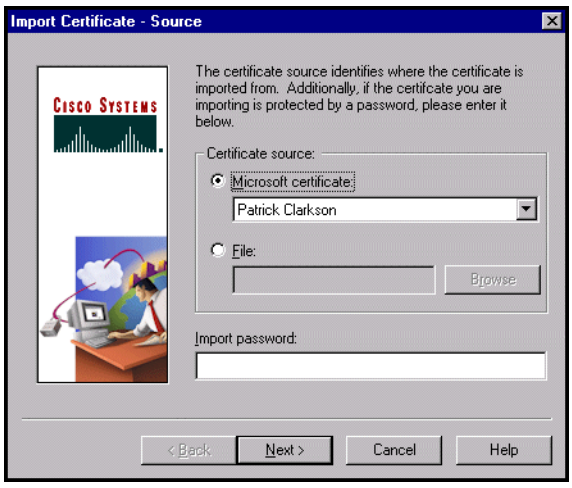
Importing a certificate file

You can import a certificate into the Cisco store from the Microsoft store or from a file. To import a certificate, use the following procedure:

1 On the Certificate Manager main window under the **Personal Certificates** tab, click the **Import** button.

The Certificate Manager displays the **Import Certificate - Source** dialog (Figure 6-16).

Figure 6-16: Importing a certificate


Import Certificate - Source
Cisco Systems
The certificate source identifies where the certificate is imported from. Additionally, if the certifcate you are importing is protected by a password, please enter it below.
Certificate source:
Microsoft certificate:
Patrick Clarkson
File:
Browse
Import password:
< Back
Next >
Cancel
Help

2 To import a certificate do one of the following depending on whether where your certificate resides:

- *Importing from the Microsoft store* — click the **Microsoft certificate** radio button and select the certificate from the drop-down menu. The certificate must already be in your Microsoft store.
- *Importing from a file* — click the **File** radio button and enter the pathname of the file into the field.

3 If a password is used to protect this certificate, type the password into the **Import Password:** field.

This is the password assigned to protect the certificate's private key.

– If you are importing from the Microsoft store, this password is the one you (or the network administrator) entered during enrollment.

– If you are importing a certificate from a file, this is the password specified when the certificate was exported.

4 Click **Next>**.

The Certificate Manager prompts for a password to be stored with the certificate (Figure 6-17).

Figure 6-17: Destination password for importing certificate

Certificate Password Protection
Cisco Systems
Password protecting your certificate provides an additional level of security. This password is optional.
By choosing to protect your certificate with a password, any operation that requires access to the certificate's private key will require the specified password to continue.
Note - File based enrollments require the password used here to be re-entered when the approved certificate is imported.
Password:
Confirmation Password:
< Back
Finish
Cancel
Help

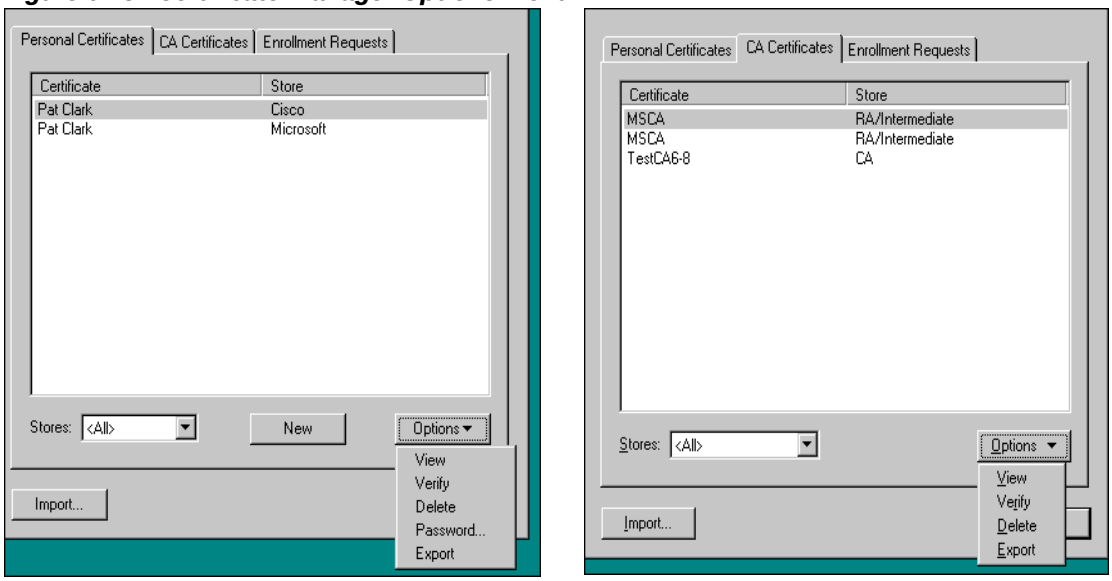
5 Type a password into the **Password** field, and click **Finish**.

This password must exactly match the password given during enrollment (online) or given when exported (if file), including upper and lower case letters. For example, *sKate8* is not exactly the same as *Skate8*. In online enrollment, this password is kept with the certificate; in file enrollment, this password is not retained.

Managing personal and CA/RA certificates

Using the Certificate Manager, you can view a certificate, verify that the certificate is still valid (within the dates assigned to it and has not been revoked), delete a certificate, and export the certificate to a file that you can email to someone. For personal certificates only, you can also change the certificate's password. To perform any of these actions, use the **Options** menu on the main window (Figure 6-18).

Figure 6-18: Certificate Manager Options menu

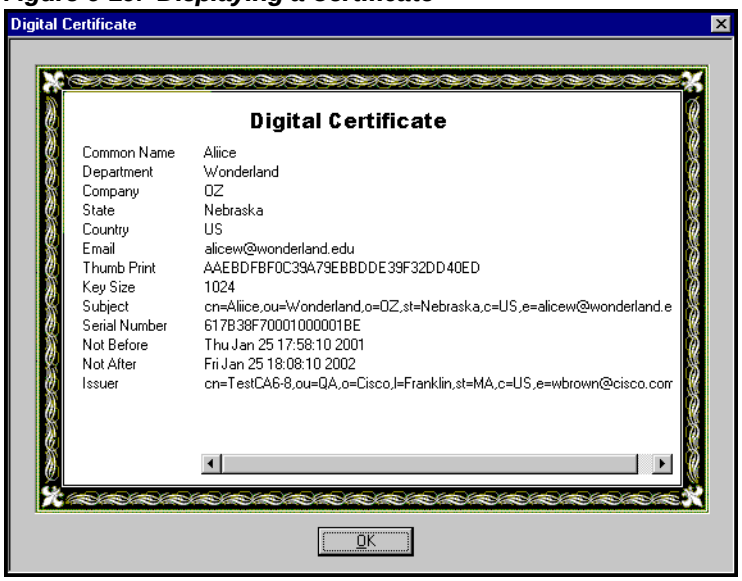


Viewing a certificate

To display a certificate, select it in the certificate store, open the **Options** pull-down menu and select **View**. Or, you can double-click on the certificate to display it.

Figure 6-19 shows a sample certificate from a Microsoft certificate service provider. This is only an example. Not all certificates are guaranteed to look like this one.

Figure 6-19: Displaying a Certificate



A typical certificate shown in Figure 6-19 contains the following information.

- **Common Name**: The name of the owner, usually the first name and last name. This field identifies the owner within the Public Key Infrastructure (PKI organization).
- **Department**: The name of the owner's department, which is same as the Organizational Unit (OU). Note that when connecting to a VPN 3000 Concentrator, the OU must match the Group Name configured for the owner in the VPN 3000 Concentrator.
- **Company**: The organization where the owner is using the certificate.
- **State**: The state where the owner is using the certificate.
- **Country**: The two-character country code where the owner's system is located.
- **Email**: The email address of the owner of the certificate.
- **Thumbprint**: An MD5 hash of the certificate's complete contents, which provides a means of validating the authenticity of the certificate. For example, you can contact the issuing CA and use this identifier to verify that this certificate is indeed the right one.
- **Key Size**: The size of the signing key pair in bits; for example, 512.
- **Subject**: The fully qualified distinguished name (DN) of certificate's owner. This specific example includes the following parts. Other items may be included, depending on the certificate type. However, these fields are fairly standard.
  - **cn** is the common name.
  - **ou** is the organizational unit (department)
  - **o** is the organization
  - **l** is the locality (city or town).
  - **st** is the state or province of the owner.
  - **c** is the country.
  - **e** is the email address of the owner.
- **Serial Number**: A unique identifier used for tracking the validity of the certificate on Certificate Revocation Lists (CRLs).
- **Not Before**: The beginning date that the certificate is valid.
- **Not After**: The end date beyond which the certificate is no longer valid.
- **Issuer**: The fully qualified distinguished name (DN) of the source that provided the certificate. The fields in this example are the same as for **Subject**.

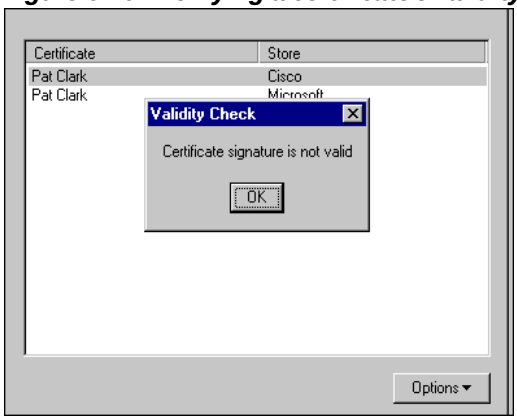
After you have finished viewing the certificate, click **OK** to close it.

Verifying a certificate

The Certificate Manager provides a quick way for you to check the validity of a certificate; for example to see if it is within the valid beginning and ending date range. To see if the certificate is valid, select it in the certificate store, display the **Options** pull-down menu, and select **Verify**.

The Certificate Manager displays a message such as the one in Figure 6-20 indicating whether the certificate is still valid.

Figure 6-20: Verifying a certificate's validity



The following table shows the messages you can might see when you check the validity of your certificate.

Message	Meaning and action
`Certificate is not valid yet`	The current date is prior to the certificate's valid start date. You must wait until the certificate becomes valid.
`Certificate has expired`	The current date is after the certificate's valid end date. You need to enroll for new certificate.
`Certificate signature is not valid`	You don't have the CA certificate, or the CA certificate that you have may have expired. You may need to download or import the CA certificate.
`Certificate is valid`	You have a working certificate enrolled.

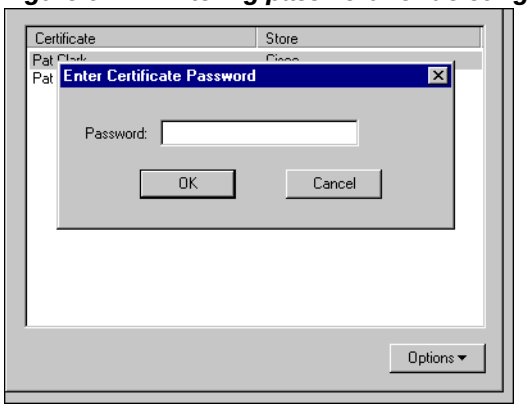
Deleting a certificate

To delete a certificate, follow this procedure:

1 **Select** the certificate in the certificate store, display the **Options** pull-down menu, and select **Delete**.

If there is a password on the certificate, the Certificate Manager prompts you to enter it (Figure 6-21).

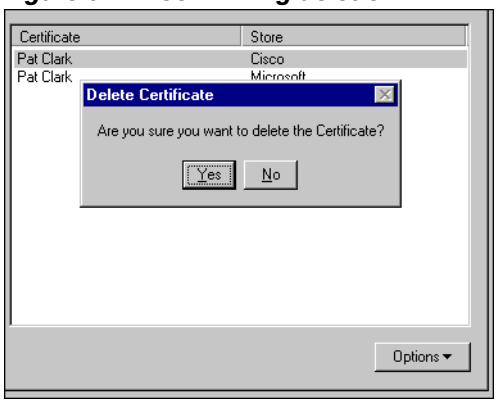
Figure 6-21: Entering password for deleting a certificate



2 In the **Password** field, type the password given to the certificate during enrollment and click **OK**.

Next, the Certificate Manager asks you to confirm (Figure 6-22).

Figure 6-22: Confirming deletion



3 To complete the deletion, click **Yes**. If you decide not to delete this certificate, click **No**.

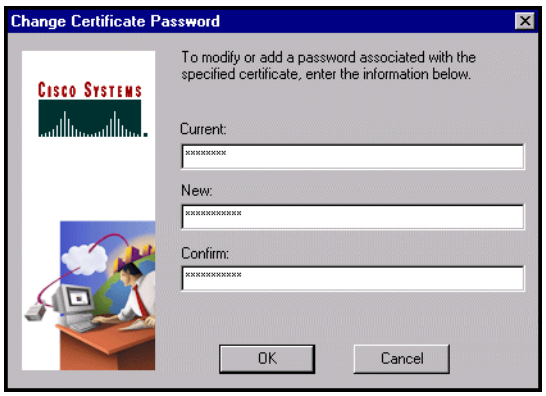
Changing the password on a personal certificate

To change the password on a personal certificate, use this procedure:

1 Display the **Options** pull-down menu and select **Password...**.

The Certificate Manager displays the Change Password dialog (Figure 6-23).

Figure 6-23: Changing a certificate's password



2 In the **Current** field, type the password you are currently using to protect your private key.

3 In the **New** field, type the new password.

4 In the **Confirm** field, type the same password again.

5 Click **OK**.

Exporting a certificate

You may want to export a certificate, primarily for backing up your certificate and private key or moving them to another system. When you export a certificate, you are making a copy of it.

To export a certificate, follow these steps:

1 Display the **Options** pull-down menu and select **Export**.

The Certificate Manager displays the Export Certificate dialog (Figure 6-24).

Figure 6-24: Exporting a certificate

Export Certificate
Cisco Systems
The certificate password is not exported with the certificate. To password protect the certificate file, enter a value in the Export password field.
To export the CA certificate (and any intermediate CA certificates), select the Export certificate chain option.
Certificate password:
Export password:
Confirm Export password:
Export file name: *
export_newcert.cec
Browse
Export certificate chain
* Required Field
OK
Cancel

2 In the **Certificate password** field, enter the password initiated during enrollment, if any.

The Certificate password protects the certificate in the certificate store (so an unauthorized individual can't use it). This is the password you optionally entered when you enrolled for the certificate.

3 In the **Export password** field, enter an optional password to protect the export file. Then enter it again in the **Confirm password** field.

4 In the **Export filename** field, enter the filename for the exported certificate. Only the filename is required. Use the **Browse** feature to locate a target directory for the exported certificate.

5 To export the CA and/or RA certificate with your personal certificate, check the **Export certificate chain** option.

6 After completing all the information, click **OK**.

The Certificate Manager displays a message indicating whether your certificate export was successful (Figure 6-25).

Figure 6-25: Export message

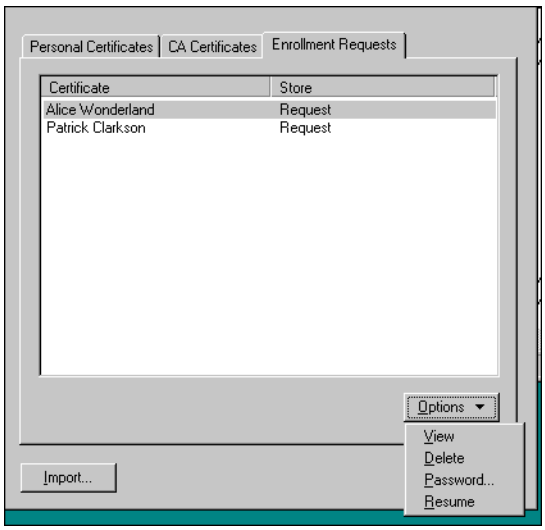
Export Certificate
The certificate password is not exported with the certificate. To password protect the certificate file, enter a value in the Export password field.
To export the CA certificate (and any intermediate CA certificates), select the Export certificate chain option.
Certificate password:
Export Success
Export of certificate was successful
OK
Export file name: *
backup_CA.p7b
Browse
Export certificate chain
* Required Field
OK
Cancel

7 To continue, click **OK**.

Managing enrollment requests

While a request is pending approval by the CA administration, the Certificate Manager places the enrollment request under the **Enrollment Requests** tab. You can view, delete, or change the password on any request in the list; or you can resume a network enrollment request. To perform any of these actions, select the **Enrollment Requests** tab and click on the **Options** pull-down menu (Figure 6-26).

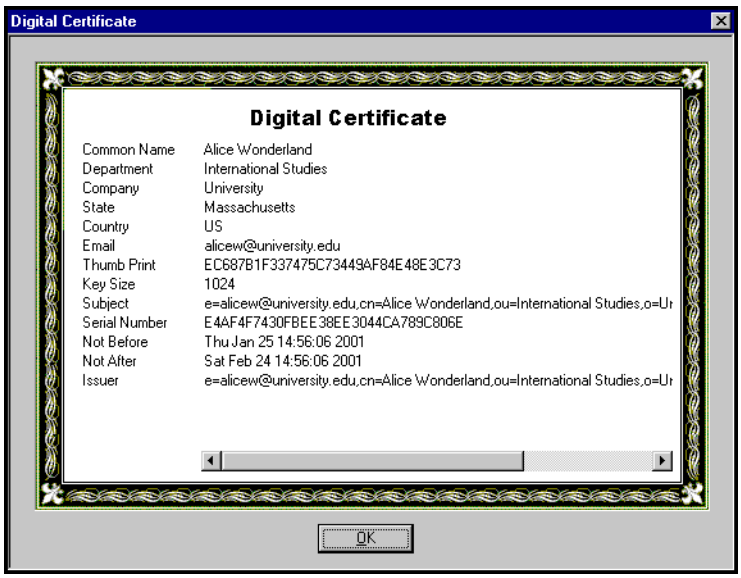
Figure 6-26: Managing enrollment requests



Viewing the enrollment request

To display the enrollment request, click on its name in the list and select **View** from the **Options** pull-down menu. The Certificate Manager displays the pending request (Figure 6-27).

Figure 6-27: Viewing an enrollment request



Note that the **Issuer** field shows the subject name and not the name of the CA, since the CA has not yet issued the certificate.

Deleting an enrollment request

To delete an enrollment request, follow these steps:

1. Click on the enrollment request in the list and select **Delete** from the **Options** pull-down menu.

   The Certificate manager prompts you for a password.

2. Type the password in the **Password** field and click **OK**.

   The Certificate Manager verifies the password. If the password is correct, the Certificate Manager asks you to confirm that you really want to delete the enrollment request.

3. To complete the deletion, click **Yes**. If you decide not to delete this certificate, click **No**.

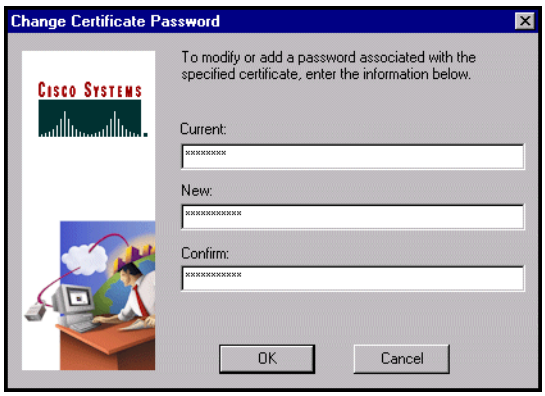
Changing the password on an enrollment request

To change the password on a certificate, use this procedure:

1. Display the **Options** pull-down menu and select **Password...**.

   The Certificate Manager displays the **Change Certificate Password** dialog (Figure 6-28).

Figure 6-28: Changing a certificate's password



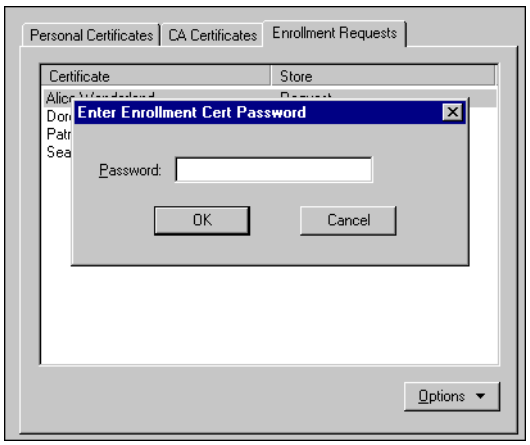
2. In the **Current** field, type the password you are currently using.
3. In the **New** field, type the new password.
4. In the **Confirm** field, type your new password again.
5. Click **OK**.

Completing an enrollment request

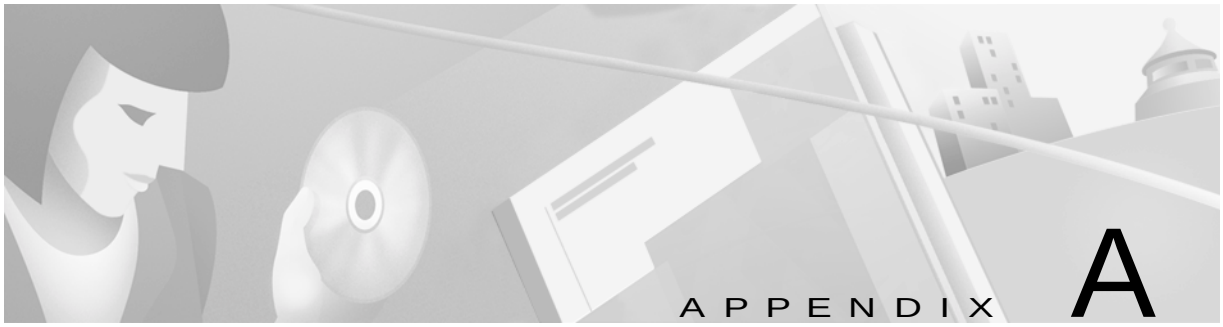
To complete a pending enrollment request, select the request under the **Enrollment Requests** tab, and select **Resume** from the **Options** pull-down menu.

The Certificate Manager prompts you to enter a password (Figure 6-29). This password must match the password you are using to protect the certificate's private key, if any.

Figure 6-29: Entering password to resume online enrollment



Enter the password and click **OK** to resume enrollment.



Copyrights and licenses

Client Software License Agreement of Cisco Systems

THE SOFTWARE TO WHICH YOU ARE REQUESTING ACCESS IS THE PROPERTY OF CISCO SYSTEMS. THE USE OF THIS SOFTWARE IS GOVERNED BY THE TERMS AND CONDITIONS OF THE AGREEMENT SET FORTH BELOW. BY CLICKING "YES" ON THIS SCREEN, YOU INDICATE THAT YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THAT AGREEMENT. THEREFORE, PLEASE READ THE TERMS AND CONDITIONS CAREFULLY BEFORE CLICKING ON "YES". IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THE AGREEMENT, CLICK "NO" ON THIS SCREEN, IN WHICH CASE YOU WILL BE DENIED ACCESS TO THE SOFTWARE.

Ownership of the Software

1. The software contained in the Cisco Systems VPN Client ("the Software"), to which you are requesting access, is owned or licensed by Cisco Systems and is protected by United States copyright laws, laws of other nations, and/or international treaties.

Grant of License

2. Cisco Systems hereby grants to you the right to install and use the Software on an unlimited number of computers, provided that each of those computers must use the Software only to connect to Cisco Systems products, and subject to export restrictions in paragraph 4 hereof. You may make one copy of the Software for each such computer for the purpose of installing the Software on that computer. The Software is licensed for use only with Cisco Systems products, and for no other use.

Restrictions on Use and Transfer

3. You may not otherwise copy the Software, except that you may make one copy of the Software solely for backup or archival purposes. To this end, you may transfer the Software to a single set of disks provided you keep the disks solely for backup or archival purposes. You may not use the backup or archival copy of the Software except in conjunction with Cisco Systems products.

4. You may not transfer the Software to any third party without the express written permission of Cisco Systems. For permitted transfers, you may not export the Software to any country for which the United States requires any export license or other governmental approval at the time of export without first obtaining the requisite license and/or approval. Furthermore, you may not export the Software in violation of any export control laws of the United States or any other country.

5. You may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from, the Software or any accompanying documentation or any copy thereof, in whole or in part.

6. The subject license will terminate immediately if you do not comply with any and all of the terms and conditions set forth herein. Upon termination for any reason, you (the licensee) must immediately destroy the Software, any accompanying documentation, and all copies thereof. Cisco Systems is not liable to you for damages in any form solely by reason of termination of this license.

7. You may not remove or alter any copyright, trade secret, patent, trademark, trade name, logo, product designation or other proprietary and/or other legal notices contained in or on the Software and any accompanying documentation. These legal notices must be retained on any copies of the Software and accompanying documentation made pursuant to paragraphs 2 and 3 hereof.

8. You shall acquire no rights of any kind to any copyright, trade secret, patent, trademark, trade name, logo, or product designation contained in, or relating to, the Software or accompanying documentation and shall not make use thereof except as expressly authorized herein or otherwise authorized in writing by Cisco Systems.

Limitation Of Liabilities

9. INSTALLATION AND USE OF THE SOFTWARE IS ALSO GOVERNED BY A SEPARATE LICENSE AGREEMENT BETWEEN CISCO SYSTEMS AND THE PURCHASER OF THE CISCO SYSTEMS VPN 3000 CLIENT PRODUCT. THAT SEPARATE LICENSE AGREEMENT CONTAINS A DESCRIPTION OF ALL WARRANTIES PROVIDED BY CISCO SYSTEMS FOR THE SOFTWARE. CISCO SYSTEMS PROVIDES NO WARRANTIES FOR THE SOFTWARE OTHER THAN THOSE SET FORTH IN THAT AGREEMENT, AND ASSUMES NO LIABILITIES WITH RESPECT TO YOUR USE OF THE SOFTWARE.

RSA software

Copyright © 1995-1998 RSA Data Security, Inc. All rights reserved. This work contains proprietary information of RSA Data Security, Inc. Distribution is limited to authorized licensees of RSA Data Security, Inc. Any unauthorized reproduction or distribution of this document is strictly prohibited.

BSAFE is a trademark of RSA Data Security, Inc.

The RSA Public Key Cryptosystem is protected by U.S. Patent #4,405,829.

A

about this manual ix
adapter card
  network 2-2
adding
  backup servers 3-14
  new connection entry 3-4
address
  backup servers 2-3
  remote server, changing 3-16
  VPN Concentrator 3-5
  VPN device 2-2
  See also IP address
algorithms
  authentication 1-3
  DES 1-3
  encryption 1-3
  HMAC 1-3
  MD5 1-3
  SHA-1 1-3
  triple-DES 1-3
Application Launcher 5-7
authentication
  algorithms 1-3
  certificate 3-6
    requirements for 2-2
  information, connection status 4-10
  internal server 1-2, 4-4
  NT Domain 1-2, 4-5
    domain name 2-3, 4-5
    password 2-3, 4-5
    username 2-3, 4-5
  RADIUS 1-2, 4-4
  RSA 1-3, 4-5
    next cardcode 4-8
    passcode 4-6
    PIN 2-3, 4-6
    username 2-3, 4-6
  SDI *see* RSA
  SecurID 1-3, 4-5
  SoftID 1-3, 4-5
  user, methods 1-2, 4-4
Authentication tab (Properties) 3-11

B

backup servers
  adding 3-14
  addresses 2-3
  disabling 3-14
  enabling 3-14
  removing 3-14
  See also remote server, VPN Concentrator
Baltimore Technologies 4-8
base 64 encoded file type 6-8
bibliography x
binary encoded file type 6-8
bytes in, connection statistics 4-10
bytes out, connection statistics 4-10

C

CA certificates 6-3
cable connection 1-2
cable modem 1-2, 4-2
Capture icon
  log viewer 5-10
CD-ROM
  installing from 2-4
certificate
  changing 3-13
  changing password 6-15
  completing the form 6-3
  deleting 6-14
  enrollment 4-8, 6-2
    file request 6-7
    network 6-5
  expiring of 4-8
  exporting 6-16
  importing 6-10
  managing 6-11
  name of 2-3, 3-3, 3-6, 4-1
  stores 6-2
  using 4-8
  verifying 6-13
  viewing 6-12
Certificate Authorities
  CA certificates tab 6-3
Certificate Authorities (CA) 4-8
  supported (list) 2-2

Certificate Manager
Options menu 6-11
overview 6-1
starting 6-1
changing
certificate 3-13
certificate password 6-15
connection entry description 3-10
connection entry properties 3-7
group name or group password 3-12
password on an enrollment request 6-19
remote server address 3-16
Cisco
certificate store 6-2
Cisco store 6-10
clearing
events display 5-14
Client IP address, connection status 4-10
cloning a connection entry 5-3
closing the VPN Client 4-11
common name
certificate enrollment 6-3
company
certificate enrollment 6-3
completing an enrollment request 6-20
configuring
automatically 5-4
connecting
before logon 5-6
to a private network 4-2, 4-3
to the internet 1-1
via Dial-Up Networking 3-14, 4-2
with certificate 4-1
connection
LAN 1-2
network, direct 2-2
statistics, resetting 4-11
status, viewing 4-9
technologies 1-2
connection entry
changing
description 3-10
properties 3-7
remote server address 3-16
cloning 5-3
creating 3-4
creating shortcut for 5-4
definition 3-1
deleting 5-3
description 3-4
changing 3-10
managing 5-2
name 3-4
optional parameters 3-7
parameters 3-1
preconfigured 3-1
properties, changing 3-7
renaming 5-4
connection statistics 4-10
bytes in 4-10
bytes out 4-10
packets bypassed 4-11
packets decrypted 4-11
packets encrypted 4-11
connection status
IPSec through NAT Mode 4-10
key icon 4-11
NAT Port 4-10
secure associations 4-11
secured routes 4-11
time connected 4-11
Connection Status dialog box 4-10
Connections tab (Properties) 3-13
conventions
documentation x
typographic x
copyrights and licenses 1
country code
certificate enrollment 6-3
creating
new connection entry 3-4
shortcut for connection entry 5-4
Cybertrust Enterprise CA 4-8

D

deleting
certificate 6-14
connection entry 5-3
enrollment request 6-19
department
certificate enrollment 6-3
DES (Data Encryption Standard) algorithm 1-3
description, connection entry 3-4
changing 3-10
dial-up modem 1-2
Dial-Up Networking 1-3
closing before uninstall 5-15
configuration information 2-3
connecting via 3-14, 4-2
icon on taskbar 4-3
phonebook entries 3-15
requirement for 2-2
User Information dialog box 4-2
dial-up networking programs
third party 3-15
direct network connection 2-2
disabling backup servers 3-14

disconnecting 4-12
Disk icon
  log viewer 5-14
diskettes, installing from 2-4
displaying
  help 3-2
  software version 3-3
documentation
  additional ix
  conventions x
domain
  Certificate Authority 6-5
domain name
  certificate enrollment 6-3
  NT Domain authentication 2-3, 4-5
DSL (Digital Subscriber Line) 1-2
DSL modem 1-2, 4-2

E

email address
  certificate enrollment 6-3
enabling
  backup servers 3-14
encryption
  algorithms 1-3
  information, connection status 4-10
enrolling
  certificates 6-2
    file request 6-7
    network 6-5
enrolling in a PKI 4-8
Enrollment form 6-3
enrollment request
  changing password 6-19
  completing 6-20
  deleting 6-19
  pasting 6-7
  resuming 6-20
  viewing 6-18
enrollment requests
  managing 6-17
Entrust Technologies 4-8
Erase icon
  log viewer 5-14
exiting the VPN Client 4-11
exporting a certificate 6-16

F

F1 button 3-2
features, software, of VPN Client 1-2
file types for certificate enrollment 6-8
Filter icon
  log viewer 5-11
filtering events
  log viewer 5-11

G

General tab (Properties) 3-10
group name (IPSec) 2-2, 3-5
  changing 3-12
group password (IPSec) 2-2, 3-5
  changing 3-12
GTE Cybertrust 4-8

H

hard disk space requirement 2-1
help
  displaying 3-2
  from program menu 3-2
Help icon
  log viewer 5-10
  program menu 3-2
  title line 3-2
HMAC (Hashed Message Authentication Coding) algorithm 1-3
hostname, VPN Concentrator 3-5
hostname, VPN device 2-2
how it works 1-2
HTML help
  displaying 3-2

I

icon
  Dial-Up Networking 4-3
  key 4-11
  VPN Client
    displays when connected 4-9
    using to disconnect 4-12
    using to view connection status 4-9
icons
  help
    program menu 3-2
    title line 3-2
  log viewer
    Capture 5-10
    Disk 5-14
    Erase 5-14
    Filter 5-11
    Help 5-10
    Printer 5-13
    Search 5-13
IKE protocol 1-2
import option 5-4

Import Password 6-11
importing a certificate file 6-10
information you need (worksheet) 2-2
installation media requirements 2-1
installing
  VPN Client 2-1
    new version 5-14
    steps 2-4
interface card, network 2-2
internal server, authentication via 1-2, 4-4
  password 4-4
  username 4-4
internet, connecting to 1-1
  via Dial-Up Networking 3-14, 4-2
Internet Key Management (IKE) protocol 1-2
Internet Protocol Security (IPSec) protocol 1-2
IP address
  certificate enrollment 6-3
IP address, VPN Concentrator 3-5
IP address, VPN device 2-2
IPSec
  group name 2-2, 3-5
    changing 3-12
  group password 2-2, 3-5
    changing 3-12
  protocol 1-2
IPSec through NAT mode 4-10
ipsecdlr.ini file
  importing into VPN Client 5-4
ISDN (Integrated Services Digital Network) 1-2
ISDN modem 4-2
ISP
  password 2-2, 4-3
  username 2-2, 4-3

K

key icon, connection status 4-11

L

LAN connection 1-2
launching an application 5-7
licenses and copyrights 1
log file
  printing 5-13
  saving 5-14
log viewer
  clearing 5-14
  event severity levels 5-11
  filtering events 5-11
  icons
    Capture 5-10
    Disk 5-14
    Erase 5-14
    Filter 5-11
    Help 5-10
    Printer 5-13
    Search 5-13
  searching 5-13
logging events to a file 3-10
logging on to Microsoft Network 3-11

M

managing
  certificates 6-1, 6-11
  connection entries 5-2
  enrollment requests 6-17
MD5 (Message Digest 5) algorithm 1-3
Microsoft
  certificate store 6-2
Microsoft 2000 certificate store 6-2
Microsoft 2000 store 6-10
Microsoft Certificate Services 4-8
Microsoft Network, logging on 3-11
Microsoft Windows 2000 4-8
modem
  cable 1-2, 4-2
  dial-up 1-2
  DSL 1-2, 4-2
  ISDN 4-2
  requirement for 2-2

N

name
  connection entry 3-4
  IPSec group 2-2, 3-5
    changing 3-12
NAT Port 4-10
network
  adapter / interface card 2-2
  connection, direct 2-2
  installing from 2-4
New Connection Entry Wizard 3-4
NT Domain authentication 1-2, 4-5
  domain name 2-3, 4-5
  password 2-3, 4-5
  username 2-3, 4-5
NT logon 5-6

O

Options menu 3-8
organization of this manual ix
Organizational Unit (OU)
  certificate enrollment 6-3

P

packets
bypassed, connection statistics 4-11
decrypted, connection statistics 4-11
discarded, connection statistics
packets discarded 4-11
encrypted, connection statistics 4-11
passcode, RSA authentication 4-6
password
internal server authentication 4-4
IPSec group 2-2, 3-5
changing 3-12
ISP logon 2-2, 4-3
NT Domain authentication 2-3, 4-5
private key 4-1
RADIUS authentication 2-3, 4-4
PIN, RSA authentication 2-3, 4-6
PKCS10 format 6-8
PKIs
supported 2-2, 4-8
POTS (Plain Old Telephone Service) 1-2
preconfigured connection entry 3-1
Printer icon
log viewer 5-13
printing
log file 5-13
private key
password 4-1
private network
connecting to 4-2, 4-3
disconnecting from 4-12
Properties dialog box 3-8
protocols
IKE 1-2
IPSec 1-2
Public Key Infrastructure *See PKI*

Q

quitting the VPN Client 4-11

R

RADIUS authentication 4-4
password 2-3, 4-4
username 2-3, 4-4
RADIUS (Remote Authentication Dial-In User Service) 1-2
RAM requirements 2-1
reconfiguring automatically 5-4
references (bibliography) x
remote access connection
closing before uninstall 5-15
remote server
backup, addresses 2-3
changing address 3-16
See also backup servers, VPN Concentrator
removing
backup servers 3-14
the VPN Client 5-15
renaming a connection entry 5-4
requirements, system 2-1
resetting connection statistics 4-11
restarting your computer after installation 2-5
resuming an enrollment request 6-20
RSA (formerly SDI)
authentication 1-3, 4-5
Next Cardcode 4-8

S

Save Password option 4-5
saving
log file 5-14
SDI *see* RSA
Search icon
log viewer 5-13
searching
log file 5-13
secure associations
connection status 4-11
secured routes
connection status 4-11
key icon 4-11
SecurID authentication 1-3, 4-5
server
See backup servers, remote server, VPN Concentrator
Server IP address
connection status 4-10
severity levels, events 5-11
SHA-1 (Secure Hash Algorithm) 1-3
shortcut, creating for connection entry 5-4
SoftID authentication 1-3, 4-5
software features of VPN Client 1-2
software license agreement 1
software token applications, launching from VPN Dialer 5-7
start before logon 5-6
starting the VPN Client 3-4, 4-1
via shortcut 5-4
state
certificate enrollment 6-3
statistics
connection 4-10
stopping the VPN Client 4-11
stores
certificate 6-2
system administrator 2-2
system requirements 2-1

T

TCP/IP requirement 2-1
Third party dail-up program 3-15
time connected
  connection status 4-11
triple-DES algorithm 1-3
tunnel 1-2
tunnel negotiation process 4-3
typographic conventions x

U

understanding the VPN Client 1-1
UniCERT 4-8
uninstalling the VPN Client 5-15
URL or Network Address
  CA 6-5
user authentication 1-2, 4-4
  See authentication
username
  internal server authentication 4-4
  ISP logon 2-2, 4-3
  NT Domain authentication 2-3, 4-5
  RADIUS authentication 2-3, 4-4
  RSA authentication 2-3, 4-6

V

verifying a certificate 6-13
viewing
  connection status 4-9
  enrollment request 6-18
viewing a certificate 6-12
VPN Client main dialog box 3-4
VPN Client version
  finding 3-3
VPN Concentrator
  authentication using internal server 1-2, 4-4
  hostname 3-5
  IP address 3-5
VPN device
  hostname 2-2
  IP address 2-2
VPN (Virtual Private Network) 1-1

W

Windows 2000 requirement 2-1
Windows 95/98, requirement 2-1
Windows ME requirement 2-1
Windows NT, requirement 2-1
Windows username and password 3-11
worksheet, information you need 2-2

X

X.509 DER file 6-8